
NOTI•FIRE•NET™ Web Server Installation/Operation Manual

Fire Alarm System Limitations

While a fire alarm system may lower insurance rates, it is not a substitute for fire insurance!

An automatic fire alarm system—typically made up of smoke detectors, heat detectors, manual pull stations, audible warning devices, and a fire alarm control with remote notification capability—can provide early warning of a developing fire. Such a system, however, does not assure protection against property damage or loss of life resulting from a fire.

The Manufacturer recommends that smoke and/or heat detectors be located throughout a protected premise following the recommendations of the current edition of the National Fire Protection Association Standard 72 (NFPA 72), manufacturer's recommendations, State and local codes, and the recommendations contained in the Guide for Proper Use of System Smoke Detectors, which is made available at no charge to all installing dealers. A study by the Federal Emergency Management Agency (an agency of the United States government) indicated that smoke detectors may not go off in as many as 35% of all fires. While fire alarm systems are designed to provide early warning against fire, they do not guarantee warning or protection against fire. A fire alarm system may not provide timely or adequate warning, or simply may not function, for a variety of reasons:

Smoke detectors may not sense fire where smoke cannot reach the detectors such as in chimneys, in or behind walls, on roofs, or on the other side of closed doors. Smoke detectors also may not sense a fire on another level or floor of a building. A second-floor detector, for example, may not sense a first-floor or basement fire.

Particles of combustion or "smoke" from a developing fire may not reach the sensing chambers of smoke detectors because:

- Barriers such as closed or partially closed doors, walls, or chimneys may inhibit particle or smoke flow.
- Smoke particles may become "cold," stratify, and not reach the ceiling or upper walls where detectors are located.
- Smoke particles may be blown away from detectors by air outlets.
- Smoke particles may be drawn into air returns before reaching the detector.

The amount of "smoke" present may be insufficient to alarm smoke detectors. Smoke detectors are designed to alarm at various levels of smoke density. If such density levels are not created by a developing fire at the location of detectors, the detectors will not go into alarm.

Smoke detectors, even when working properly, have sensing limitations. Detectors that have photoelectronic sensing chambers tend to detect smoldering fires better than flaming fires, which have little visible smoke. Detectors that have ionizing-type sensing chambers tend to detect fast-flaming fires better than smoldering fires. Because fires develop in different ways and are often unpredictable in their growth, neither type of detector is necessarily best and a given type of detector may not provide adequate warning of a fire.

Smoke detectors cannot be expected to provide adequate warning of fires caused by arson, children playing with matches (especially in bedrooms), smoking in bed, and violent explosions (caused by escaping gas, improper storage of flammable materials, etc.).

Heat detectors do not sense particles of combustion and alarm only when heat on their sensors increases at a predetermined rate or reaches a predetermined level. Rate-of-rise heat detectors may be subject to reduced sensitivity over time. For this reason, the rate-of-rise feature of each detector should be tested at least once per year by a qualified fire protection specialist. *Heat detectors are designed to protect property, not life.*

IMPORTANT! Smoke detectors must be installed in the same room as the control panel and in rooms used by the system for the connection of alarm transmission wiring, communications, signaling, and/or power. If detectors are not so located, a developing fire may damage the alarm system, crippling its ability to report a fire.

Audible warning devices such as bells may not alert people if these devices are located on the other side of closed or partly open doors or are located on another floor of a building. Any warning device may fail to alert people with a disability or those who have recently consumed drugs, alcohol or medication. Please note that:

- Strobes can, under certain circumstances, cause seizures in people with conditions such as epilepsy.
- Studies have shown that certain people, even when they hear a fire alarm signal, do not respond or comprehend the meaning of the signal. It is the property owner's responsibility to conduct fire drills and other training exercise to make people aware of fire alarm signals and instruct them on the proper reaction to alarm signals.
- In rare instances, the sounding of a warning device can cause temporary or permanent hearing loss.

A fire alarm system will not operate without any electrical power. If AC power fails, the system will operate from standby batteries only for a specified time and only if the batteries have been properly maintained and replaced regularly.

Equipment used in the system may not be technically compatible with the control. It is essential to use only equipment listed for service with your control panel.

Telephone lines needed to transmit alarm signals from a premise to a central monitoring station may be out of service or temporarily disabled. For added protection against telephone line failure, backup radio transmission systems are recommended.

The most common cause of fire alarm malfunction is inadequate maintenance. To keep the entire fire alarm system in excellent working order, ongoing maintenance is required per the manufacturer's recommendations, and UL and NFPA standards. At a minimum, the requirements of Chapter 7 of NFPA 72 shall be followed. Environments with large amounts of dust, dirt or high air velocity require more frequent maintenance. A maintenance agreement should be arranged through the local manufacturer's representative. Maintenance should be scheduled monthly or as required by National and/or local fire codes and should be performed by authorized professional fire alarm installers only. Adequate written records of all inspections should be kept.

Installation Precautions

Adherence to the following will aid in problem-free installation with long-term reliability:

WARNING - Several different sources of power can be connected to the fire alarm control panel. Disconnect all sources of power before servicing. Control unit and associated equipment may be damaged by removing and/or inserting cards, modules, or interconnecting cables while the unit is energized. Do not attempt to install, service, or operate this unit until this manual is read and understood.

CAUTION - *System Reacceptance Test after Software Changes.* To ensure proper system operation, this product must be tested in accordance with NFPA 72 Chapter 7 after any programming operation or change in site-specific software. Reacceptance testing is required after any change, addition or deletion of system components, or after any modification, repair or adjustment to system hardware or wiring.

All components, circuits, system operations, or software functions known to be affected by a change must be 100% tested. In addition, to ensure that other operations are not inadvertently affected, at least 10% of initiating devices that are not directly affected by the change, up to a maximum of 50 devices, must also be tested and proper system operation verified.

This system meets NFPA requirements for operation at 0-49° C/32-120° F and at a relative humidity of 85% RH - 93% per ULC - (non-condensing) at 30° C/86° F. However, the useful life of the system's standby batteries and the electronic components may be adversely affected by extreme temperature ranges and humidity. Therefore, it is recommended that this system and all peripherals be installed in an environment with a nominal room temperature of 15-27° C/60-80° F.

Verify that wire sizes are adequate for all initiating and indicating device loops. Most devices cannot tolerate more than a 10% I.R. drop from the specified device voltage.

Like all solid state electronic devices, this system may operate erratically or can be damaged when subjected to lightning-induced transients. Although no system is completely immune from lightning transients and interferences, proper grounding will reduce susceptibility. *Overhead or outside aerial wiring is not recommended, due to an increased susceptibility to nearby lightning strikes.* Consult with the Technical Services Department if any problems are anticipated or encountered.

Disconnect AC power and batteries prior to removing or inserting circuit boards. Failure to do so can damage circuits.

Remove all electronic assemblies prior to any drilling, filing, reaming, or punching of the enclosure. When possible, make all cable entries from the sides or rear. Before making modifications, verify that they will not interfere with battery, transformer, and printed circuit board location.

Do not tighten screw terminals more than 9 in-lbs. Over-tightening may damage threads, resulting in reduced terminal contact pressure and difficulty with screw terminal removal.

Though designed to last many years, system components can fail at any time. This system contains static-sensitive components. Always ground yourself with a proper wrist strap before handling any circuits so that static charges are removed from the body. Use static-suppressive packaging to protect electronic assemblies removed from the unit.

Follow the instructions in the installation, operating, and programming manuals. These instructions must be followed to avoid damage to the control panel and associated equipment. FACP operation and reliability depend upon proper installation by authorized personnel.

FCC Warning

WARNING: This equipment generates, uses, and can radiate radio frequency energy and if not installed and used in accordance with the instruction manual, may cause interference to radio communications. It has been tested and found to comply with the limits for class A computing device pursuant to Subpart B of Part 15 of FCC Rules, which is designed to provide reasonable protection against such interference when operated in a commercial environment. Operation of this equipment in a residential area is likely to cause interference, in which case the user will be required to correct the interference at his own expense.

Canadian Requirements

This digital apparatus does not exceed the Class A limits for radiation noise emissions from digital apparatus set out in the Radio Interference Regulations of the Canadian Department of Communications.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la classe A prescrites dans le Règlement sur le brouillage radioélectrique édicté par le ministère des Communications du Canada.

Acclimate Plus™, HARSH™, NOTIFIRE•NET™, ONYX™, and VeriFire™ are trademarks, and FlashScan® and VIEW® are registered trademarks of NOTIFIER. NION™ and UniNet® are trademarks of NIS. NIST™ and Notifier Integrated Systems™ are trademarks and NOTIFIER® is a registered trademark of Fire•Lite Alarms, Inc. Echelon® is a registered trademark and LonWorks™ is a trademark of Echelon Corporation. ARCNET® is a registered trademark of Datapoint Corporation. Microsoft® and Windows® are registered trademarks of the Microsoft Corporation. LEXAN® is a registered trademark of GE Plastics, a subsidiary of General Electric Company.

Precau-L-4-2002.p65

Table of Contents

SECTION ONE: NFN WEB SERVER FEATURES	7
1.1 PRODUCT DESCRIPTION	7
1.2 NFN WEB SERVER/SERIAL CONFIGURATION TOOL FEATURES	7
1.3 RELATED DOCUMENTATION	7
Table 1.3-1: Related Documentation	7
1.4 STANDARDS AND SPECIFICATIONS	8
1.5 COMPATIBILITY	8
1.6 SYSTEM REQUIREMENTS	8
1.7 SYSTEM ARCHITECTURE	9
Figure 1.7-1: NFN Web Server Network Architecture	9
Figure 1-7.2: NFN Web Server PPP Architecture	10
Figure 1-7.3: NFN Web Server Direct Panel Interface Architecture	11
SECTION TWO: NFN WEB SERVER HARDWARE INSTALLATION	13
2.1 REQUIRED COMPONENTS	13
2.2 INSTALLATION OVERVIEW	14
Figure 2.2-1: NFN Web Server Assembly Checklist	14
2.3 INSTALLING THE NFN WEB SERVER ASSEMBLY INTO A CAB-4 SERIES CABINET	15
Figure 2.3-1: NFN Web Server Installation Diagram	15
2.4 NFN WEB SERVER PC BOARD LAYOUT	15
Figure 2.4-1: PC Board Layout	15
2.5 POWER SUPPLY CONNECTIONS	16
Figure 2.5-1: 46175 Power Supply Specifications	16
Figure 2.5-2: NFN Web Server Power Connection	16
Figure 2.5-3: NWS Power Supply Connections for Direct Panel Interfacing	17
2.6 DB-9 TO NUP CONNECTION (NFN WEB SERVER TO NCM-W/F OR NUP DIRECT CONNECT)	18
Figure 2.6-1: DB-9 to NUP Connection	18
2.7 MODEM CONNECTION (NFN WEB SERVER TO MODEM)	18
Figure 2.7-1: 10-Pin to DB-9 Connection (Modem Connection)	18
2.8 ETHERNET NETWORK CONNECTION	19
Figure 2.8-1: Ethernet Connection	19
2.9 PC TO PC CONNECTION	19
Figure 2.9-1: PC to PC Serial Connection	19
SECTION THREE: NFN WEB SERVER CONFIGURATION	21
3.1 NFN WEB SERVER SERIAL CONFIGURATION TOOL INSTALLATION	21
3.2 USING THE NWS CONFIGURATION TOOL FOR CONFIGURATION	21
Figure 3.2-1: NFN Web Server Serial Setup Dialog	21
Figure 3.2-2: NFN Web Server Configuration	22
3.3 USING VERI•FIRE™ TOOLS FOR CONFIGURATION	23
Figure 3.3-1: Serial Port Configuration Utility	23
3.4 INITIAL SETUP OF THE NFN WEB SERVER	24
Figure 3.4-1: Veri•Fire™ Local Connection Type	24
Figure 3.4-2: Nodes Screen	24
Figure 3.4-3: NFN Web Server Configuration Settings	25
Figure 3.4-4: Selecting the Connection Type	26
Figure 3.4-5: Configuring the Web Server Connection Session	26
Figure 3.4-6: Veri•Fire™ Tools System Password	27
Figure 3.4-7: Selecting the Connection Type	27
Figure 3.4-8: Changing the Node Address	28
Figure 3.4-9: Changing the Node Address	28

SECTION FOUR: NFN WEB SERVER OPERATION	29
4.1 NFN WEB SERVER SECURITY	29
Figure 4.1-1: NFN Web Server Login Dialog	29
4.2 THE BROWSER INTERFACE	29
Figure 4.2-1: NWS Home Page	29
4.3 SYSTEM ADMINISTRATION	30
4.3.1 Auto Detect Points on all Panels	30
Figure 4.3.1-1: Auto Detect Points	30
Figure 4.3.1-2: Auto Point Detect AFP400 Message	31
Figure 4.3.1-3: Auto Detect Screen	31
4.3.2 E-mail Notification	32
Figure 4.3.2-1: E-mail Configuration	32
Figure 4.3.2-2: E-mail Profile Configuration	33
Figure 4.3.2-3: Email Configuration - Custom Messages	34
Figure 4.3.2-4: Sample Email Message	34
4.3.3 System Settings	35
Figure 4.3.3-1 System Settings	35
4.3.4 Monitoring Profiles	36
Figure 4.3.4-1: Monitoring Profiles	36
4.3.5 Node Mapping	37
Figure 4.3.5-1: Node Mapping	37
4.3.6 Password Configuration	38
Figure 4.3.6-1: User Configuration	38
4.3.7 Authorization Log	39
Figure 4.3.7-1: Authorization Log	39
4.4 MULTIPLE EVENT LIST	40
Figure 4.4-1: Event List Summary	40
Figure 4.4-2: Multiple Event List Details	41
4.5 VERSION INFORMATION	42
Figure 4.5-1: Version Information	42
4.6 NUP PORT STATISTICS	43
Figure 4.6-1: NUP Port Statistics Overview	43
Figure 4.6-2: Local Node NUP Port Statistics	43
4.7 SCREEN DETAILS AND OPTIONS FOR SPECIFIC PANELS	44
Figure 4.7-1: Panel Properties Display Sample	44
Figure 4.7-2: Loop Properties Sample Screen	45
Figure 4.7-3: Module Properties Sample Screen	45
Figure 4.7-4: Detector Properties Sample Screen	46
INDEX	47

NOTES

SECTION ONE: NFN WEB SERVER FEATURES

1.1 PRODUCT DESCRIPTION

The **NOTI•FIRE•NET™** Web Server is a web-based device that acts as an HTML server that allows remote access to the **NOTI•FIRE•NET™** network via the Internet or an Intranet. With the NFN Web Server interface, the user can view the history of a fire alarm control panel (FACP), event status, device properties, and other information based on access permissions defined by the system administrator. All data available on the web server is a “snapshot” of the data on the **NOTI•FIRE•NET™** network at the time the browser requested the information. The NFN Web Server communicates to **NOTI•FIRE•NET™** version 5.0 and later. The NFN Web Server interfaces to the Internet/Intranet using an IP-based wire Ethernet connection or through a direct dial-up connection using a modem. The Serial Configuration Tool allows you to make the necessary network configuration settings for the web server to be able to communicate with the browser.

1.2 NFN WEB SERVER/SERIAL CONFIGURATION TOOL FEATURES

Below are some of the features of the NFN Web Server and Serial Configuration Tool

- Ability to access **NOTI•FIRE•NET™** device and system statuses and properties remotely via the Internet, Intranet or direct dial-up connection.
- Compatible with **NOTI•FIRE•NET™** version 5.0 and later
- Serial Configuration Tool runs on any laptop or PC using Windows™ and having an open COM port
- One web server supports multiple users
- Standard IP over Ethernet connection
- Up to 128 user accounts are supported
- Built-in password security and user access record
- Supports standard Microsoft® Internet Explorer 5
- Intuitive Explorer user interface
- Sends up to 50 emails in response to any system event

1.3 RELATED DOCUMENTATION

Below is a list of **NOTI•FIRE•NET™** related documentation.

For information on...	Refer to...	Part No.
Compatible Devices	Device Compatibility Document	15378
Cabinets & Chassis	CAB-3/CAB-4 Series Installation Document	15330
Auxiliary Power Supplies & Battery Chargers	ACPS-2406 Installation Manual	51304
Offline Programming Utility	Veri•Fire™ Tools on-line help file Veri•Fire™ Medium Systems on-line help file Veri•Fire™ Tools CD Insert	VeriFire-TCD VeriFire-CD 51871
VeriFire-TCDNetworking	Noti•Fire•Net™ Manual	51584
	NCM-W/F Installation Document	51533
	MIB Media Interface Board	50255
	NCS Network Control Station	51095
	NCA Network Control Annunciator	51482
Panels and Annunciators	BACnet Gateway	51659
	NFS-640 Installation/Operation/Programming manuals	51332/51334/51333
	NFS-3030 Installation/Operation/Programming manuals	51330/51344/51345
	Network Control Annunciator (NCA)	51482
	Network Control Station (NCS)	51095
	AFP-200 Instruction manual	15511
	AFP-300/400 Installation/Operation/Programming manuals	50253/50260/50259
	AM2020/AFP1010 Installation/Operation/Programming manuals	15088
	UniNet Online Instruction Manual	51994

Table 1.3-1: Related Documentation

1.4 STANDARDS AND SPECIFICATIONS

The NFN Web Server has been designed to comply with standards set forth by the following regulatory agencies:

- Underwriters Laboratories Standard UL 864
- NFPA 72 National Fire Alarm Code
- CAN/ULC - S527-M99 Standard for Control Units for Fire Alarm Systems
- UL-1076 Proprietary Burglar Alarm Units and Systems.

The contents of this manual are important and must be kept in close proximity of the hardware. If building ownership is changed, this manual and all other testing and maintenance information must also be passed to the current owner of the facility. A copy of this manual was shipped with the equipment and is also available from the manufacturer.

WARNING: *Improper installation, maintenance, or lack of routine testing could result in system malfunction.*

1.5 COMPATIBILITY

The NFN Web Server is compatible with **NOTI•FIRE•NET™** version 5.0 and later of the following panels and devices:

- NFS-640 (version 2.0, NCM-W/F)
- NFS-3030 (version 2.0, NCM-W/F)
- AM2020 (version 5.0 SIB)
- AFP-1010 (version 5.0 SIB)
- AFP-200 (version 5.0, NAM, events only)
- AFP-300/400 (version 5.0, NAM)
- BACnet Gateway (version 2.0, events only)
- NFN NION (events only)
- Network Control Station (NCS, version 3.0, events only)
- Network Control Annunciator (NCA, version 2.0, NCM-W/F, events only)



NOTES: The NFN Web Server is not intended as a primary annunciator and is ancillary in nature.

No NCM is required when the NFN Web Server connects directly to an NFS-640 and NFS-3030.

1.6 SYSTEM REQUIREMENTS

BROWSER

- Microsoft® Internet Explorer version 5.0 or later, running on Windows 98® or Windows 2000®



NOTE: Netscape® is not supported by the NFN Web Server application.

VERI•FIRE™ TOOLS/SERIAL CONFIGURATION TOOL

- Windows 2000® operating system



NOTE: The NFN Web Server is compatible with Veri•Fire™ Tools version 3.00 or later.

DIAL-UP MODEM CONNECTION

- Serial modem with minimum capability of 57.6K baud

1.7 SYSTEM ARCHITECTURE

There are three network options for the NFN Web Server:

- Internet or Intranet connection
- Using a dial-up modem
- Direct panel interface to an NFS-640 or NFS-3030

The following diagrams show architecture options for a system using the NFN Web Server.

INTERNET/INTRANET CONNECTION

The NFN Web Server can use an Internet/Intranet connection via IP over Ethernet.

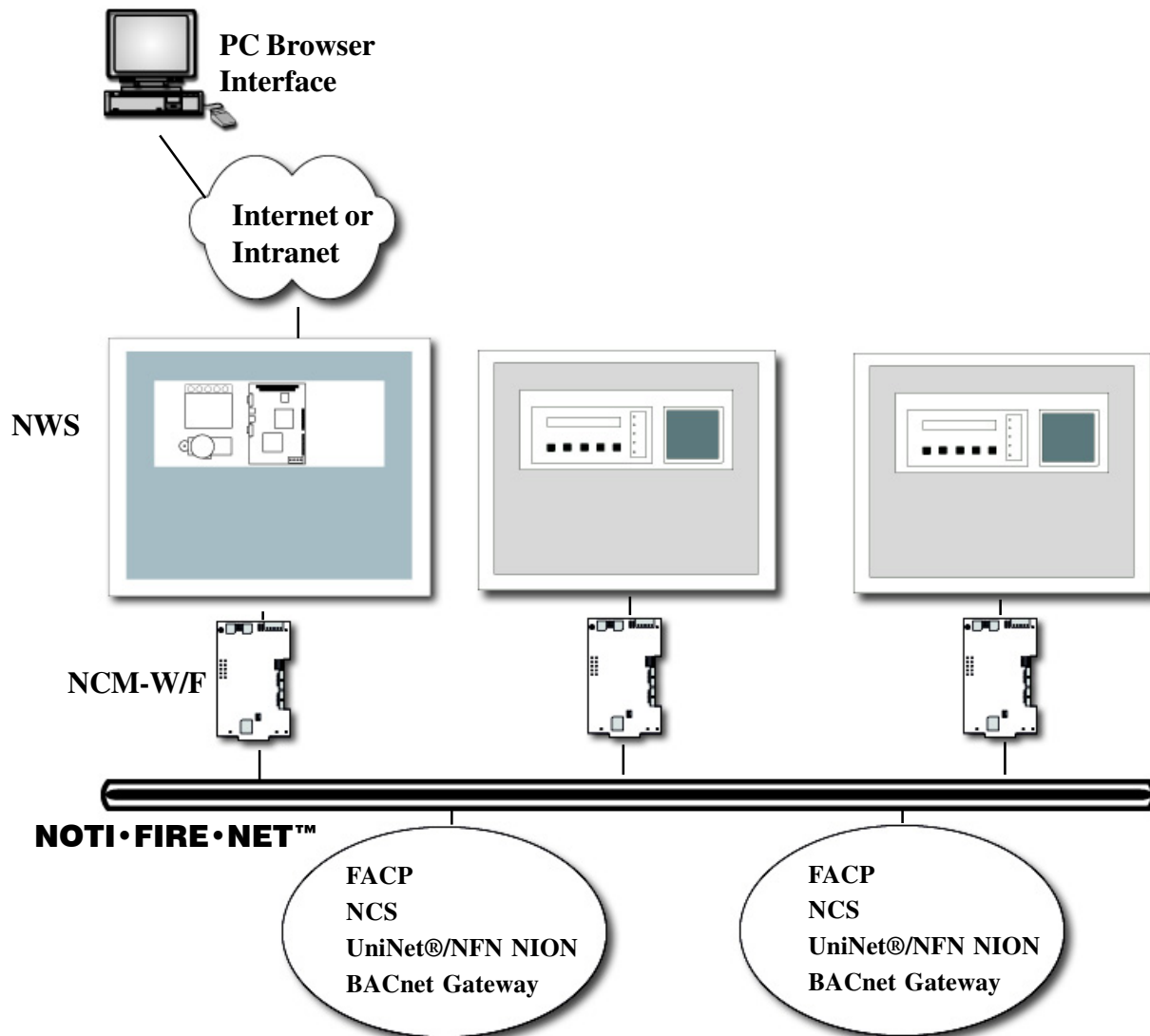


Figure 1.7-1: NFN Web Server Network Architecture

NFN WEB SERVER DIALUP CONNECTION

The NFN Web Server can use a serial modem to communicate with a remote browser via telephone lines.

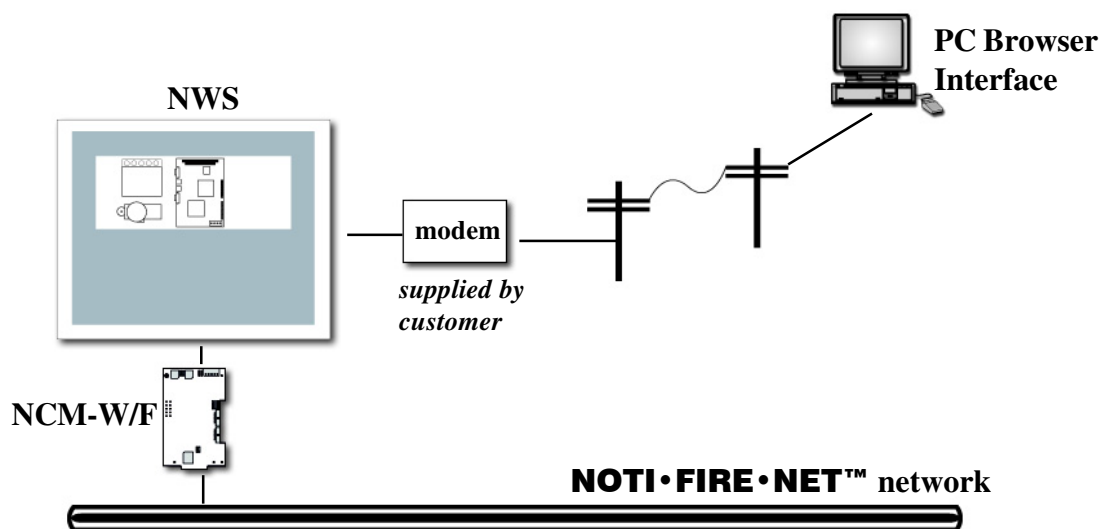


Figure 1-7.2: NFN Web Server PPP Architecture

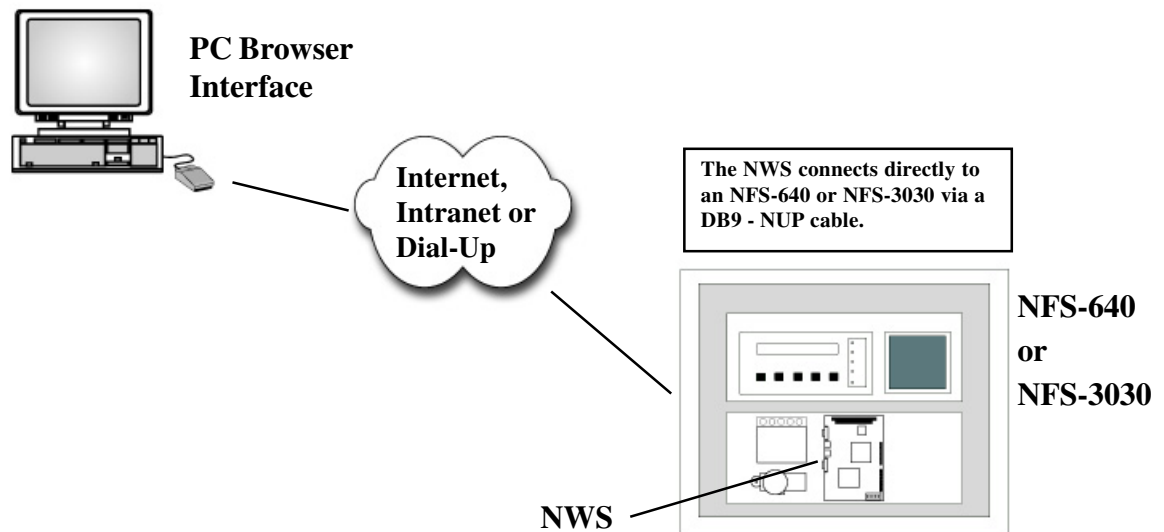


NOTES: Only one user can dial into the server at a time.

The server can support an intranet/internet connection simultaneously with a dialup connection.

NFN WEB SERVER INTERFACE TO STANDALONE PANEL (NFS-640 or NFS-3030)

The NFN Web Server can directly interface with an NFS-640 or NFS-3030 panel to connect them via Internet/Intranet to a PC browser. A DB-9-to-NUP cable is used to make the connection.



NOTE: No NCM is required when the NWS connects directly to an NFS-640 or NFS-3030.

Figure 1-7.3: NFN Web Server Direct Panel Interface Architecture

NOTES

SECTION TWO: NFN WEB SERVER HARDWARE INSTALLATION

2.1 REQUIRED COMPONENTS

The NFN Web Server requires the following equipment:

NFN Web Server Assembly:

- PC board (P/N 46173) for the NFN Web Server
- Power supply (P/N 46175) - 24VDC to 5VDC
- PNET-1 surge suppressor
- CAT5 cable (P/N 75585) - provides Ethernet connection cable between NFN Web Server PC board and PNET-1 surge suppressor
- DB9 to NUP Cable (P/N 75554) - connects the NFN Web Server to an NCM-W/F
- Modem cable - connects the Web Server to a modem (see Figure 2.7-1)
- NUP to 24V power cable (P/N 75583) - provides power for the NCM-W/F (not required for standalone mode)
- HDD Power connector (P/N 75581) - used for 24VDC to 5VDC power connection
- Serial Configuration Tool software (supplied on CD-ROM, P/N NWS-SW)
- NFN Web Server/Power Supply Mounting Plate (P/N 18541)



NOTE: The NWS is for ancillary use only and does not increase the burglary grade of service for the system.

Network Interface (sold separately):

- NCM-W/F Network Communications Module - used to facilitate network communication between the NFN Web Server and **NOTI•FIRE•NET™**. *NOTE: The NCM-W/F is not required when directly connecting an NFN Web Server to an NFS-640 or NFS-3030 when either acts as a standalone panel.*

Cabinetry/Installation Hardware (sold separately):

- CAB-3/CAB-4 series cabinet
- CHS-4L chassis

Other Required Equipment (*NOTE: These items must be supplied by the customer.*):

- PC to PC connector cable - connects the NFN Web Server to a PC or laptop.
- PC or notebook - used to configure the NFN Web Server.

2.2 INSTALLATION OVERVIEW

Use the following checklist as a guideline for assembling the hardware and making necessary cable connections. The sections that follow provide details on making these connections.

NFN Web Browser Assembly Checklist	
Hardware Assembly	
Install NFN Web Server PC board onto mounting plate	<input type="checkbox"/>
Install power supply onto mounting plate	<input type="checkbox"/>
Install PNET-1 onto mounting plate	<input type="checkbox"/>
Install mounted NFN Web Server assembly into cabinet	<input type="checkbox"/>
Install NCM-W/F - not required for direct connection	<input type="checkbox"/>
Cable Connections	
Web Server serial connection to NCM-W/F or panel CPU (P/N 75554)	<input type="checkbox"/>
Web Server power connection (P/N 75581)	<input type="checkbox"/>
Web Server network connection	<input type="checkbox"/>
PNET-1 surge suppressor connection (P/N 75585)	<input type="checkbox"/>
NCM-W/F power connection (P/N 75583) - not required for direct connection	<input type="checkbox"/>
NCM-W/F data connection	<input type="checkbox"/>

Figure 2.2-1: NFN Web Server Assembly Checklist

CAUTION: Different sources of power are used in conjunction with the NFN Web Server product. Disconnect all sources of power before servicing. This device and associated equipment may be damaged by removing and/or inserting cards, modules or interconnecting cables while this unit is powered. This damage may adversely affect the operation of this unit, but its effect may not be readily apparent.

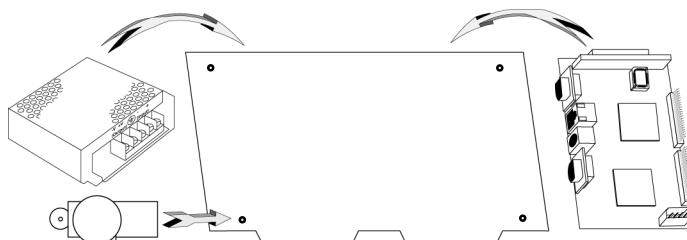
2.3 INSTALLING THE NFN WEB SERVER ASSEMBLY INTO A CAB-4 SERIES CABINET

This section describes the installation of the NFN Web Server Assembly into a CAB-3/CAB-4 series cabinet.



NOTE: Cabinet is ordered separately. For installation details, refer to the CAB-3/CAB-4 Series Installation Document, 15330.

1. The NFN Web Server, power supply and PNET-1 surge suppressor are installed onto the mounting plate. The Web Server board uses four standoffs, the power supply uses two screws, and the PNET-1 uses one.



2. The mounting plate is installed onto the CHS-4(L).

3. The CHS-4(L) is installed into the CAB-3 or CAB-4 series cabinet.

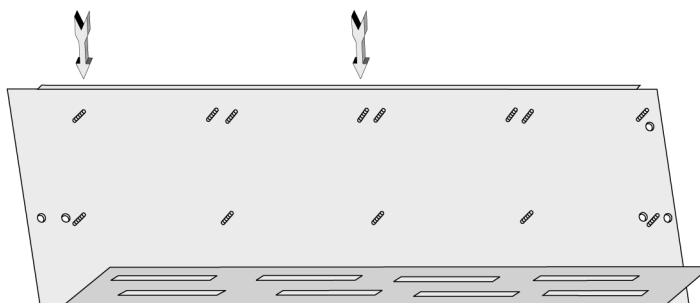


Figure 2.3-1: NFN Web Server Installation Diagram

2.4 NFN WEB SERVER PC BOARD LAYOUT

The PC board layout (P/N 46173) is shown in Figure 2.4-1 below. Descriptions of pertinent connections are described in subsequent sections.

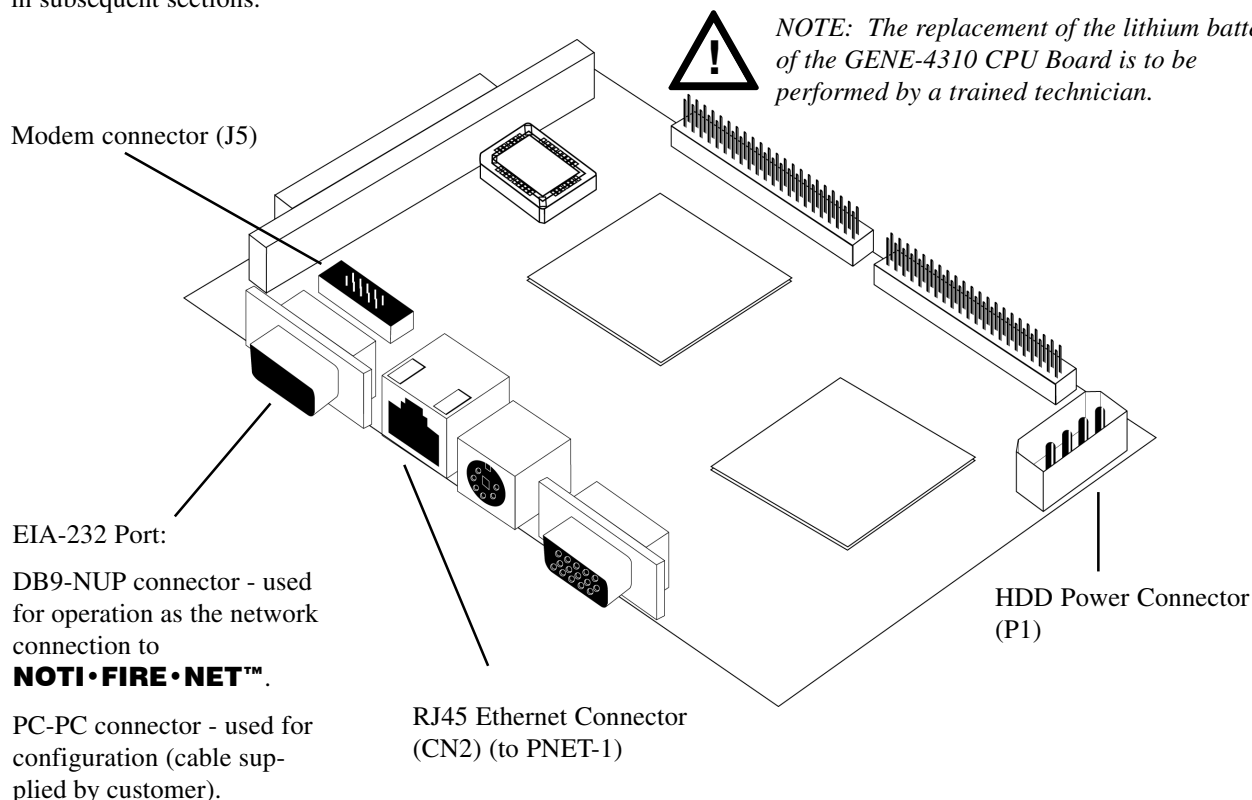


Figure 2.4-1: PC Board Layout

2.5 POWER SUPPLY CONNECTIONS

The power supply for the NFN Web Server is a 24VDC-to-5VDC unit (P/N 46175). The NFN Web Server requires +24VDC @ 250 mA nominal and battery backup in accordance with local code requirements. It can be powered by any power limited source that is UL listed for use with fire protective signaling units. For more details on powering and connecting an NCM-W/F, refer to its Product Installation Document 51533.

	TYPICAL	MIN	MAX
Input Voltage	24V	19V	29V
Input Current @24V			360mA without NCM 450 mA with NCM
Output Voltage	5V	4.8V	5.2V
Output Current @5V			1.2A

Figure 2.5-1: 46175 Power Supply Specifications

NWS POWER SUPPLY CONNECTIONS WHEN USING THE NCM-W/F

When connecting the NWS to **NOTI•FIRE•NET™** via the NCM-W/F, make cable connections according to Figure 2.5-2 below.

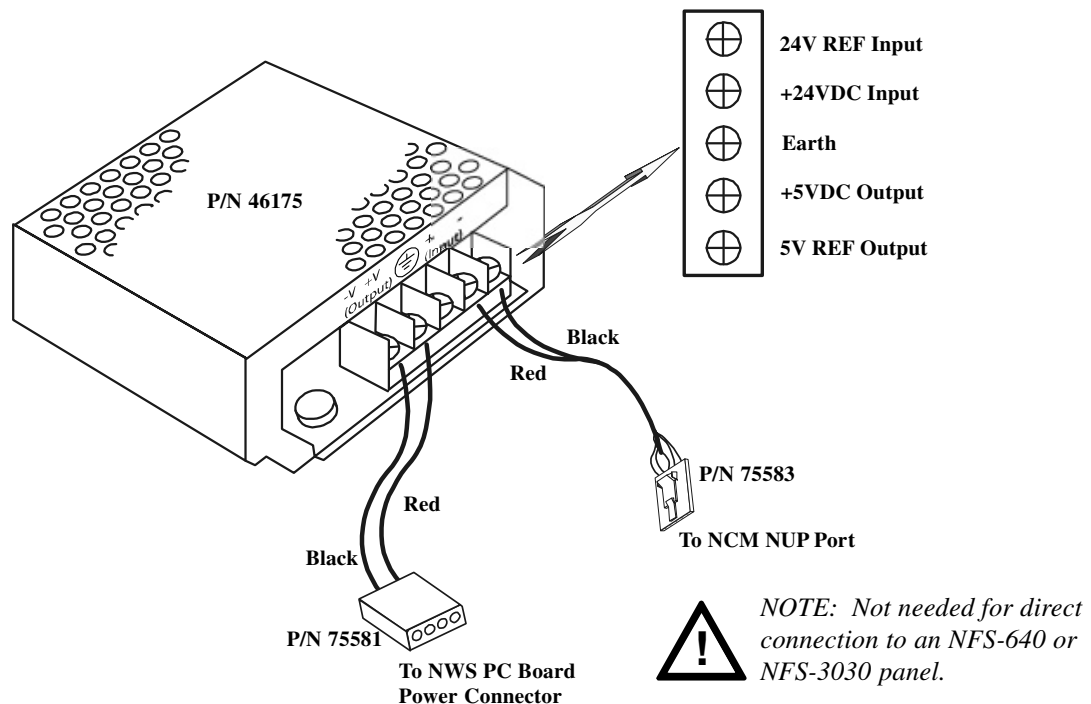


Figure 2.5-2: NFN Web Server Power Connection

NWS POWER SUPPLY CONNECTIONS WHEN CONNECTING DIRECTLY TO THE NFS-640 OR NFS-3030

When connecting the NWS directly to an NFS-640 or NFS-3030, make cable connections according to Figure 2.5-3 below.

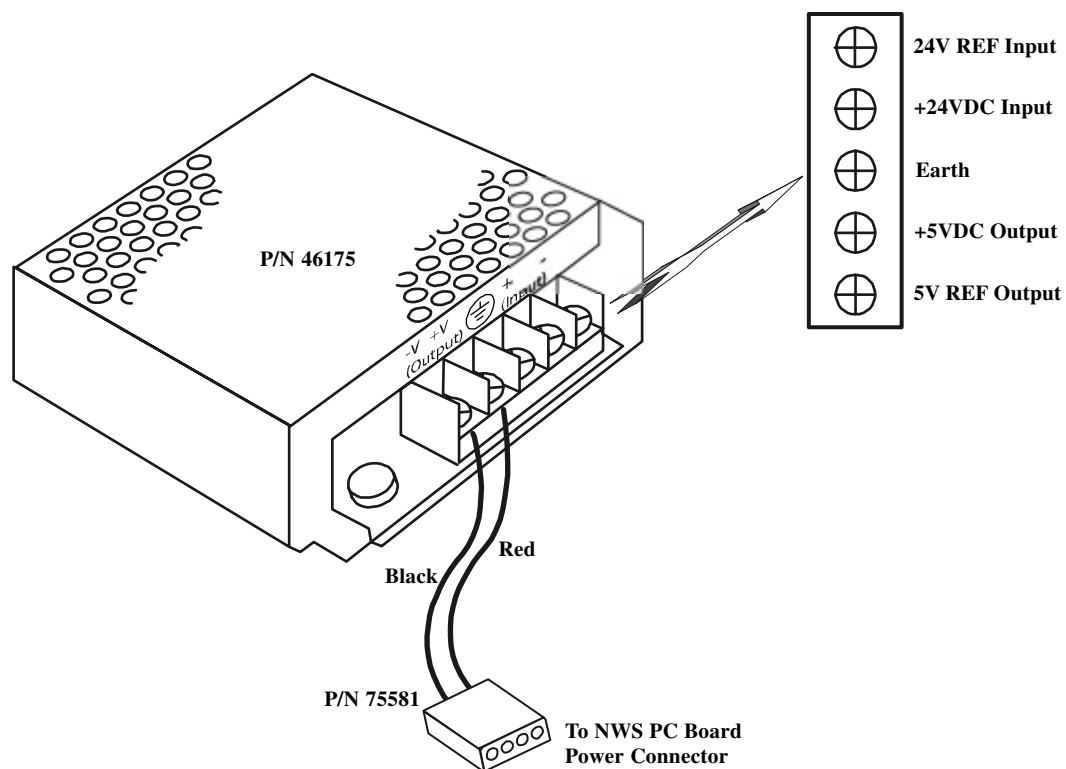


Figure 2.5-3: NWS Power Supply Connections for Direct Panel Interfacing

2.6 DB-9 TO NUP CONNECTION (NFN WEB SERVER TO NCM-W/F OR NUP DIRECT CONNECT)

Connecting the NFN Web Server to an NCM-W/F allows the Web Server to communicate with devices on the **NOTI•FIRE•NET™** network. Use the NCM-W with twisted pair wire and the NCM-F with fiber-optic cable. The NFN Web Server can also connect directly to an NFS-640 or NFS-3030 panel via the NUP port on the CPU-640 or CPU-3030. Make connections according to Figure 2.6-1 below:

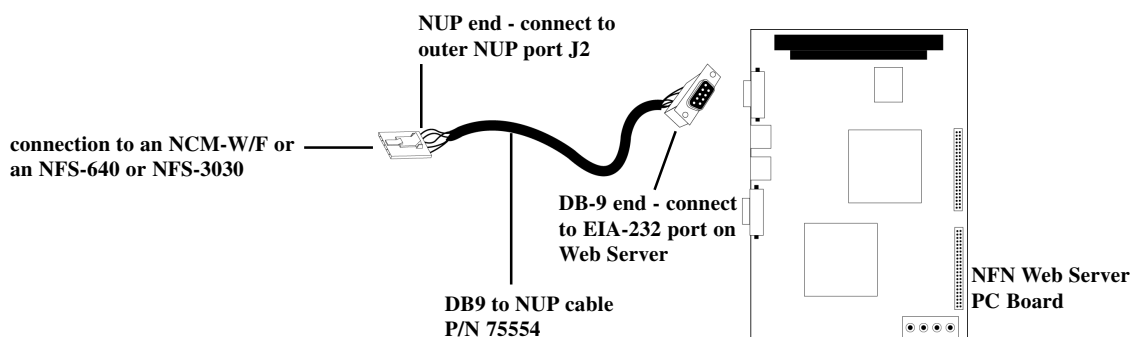


Figure 2.6-1: DB-9 to NUP Connection

2.7 MODEM CONNECTION (NFN WEB SERVER TO MODEM)

You can connect the NFN Web Server to a modem, allowing communication between the server and the browser via telephone lines. The modem must be supplied by the customer; the cable comes with the NFN Web Server PC board.



NOTE: The modem used must be ITE listed equipment.

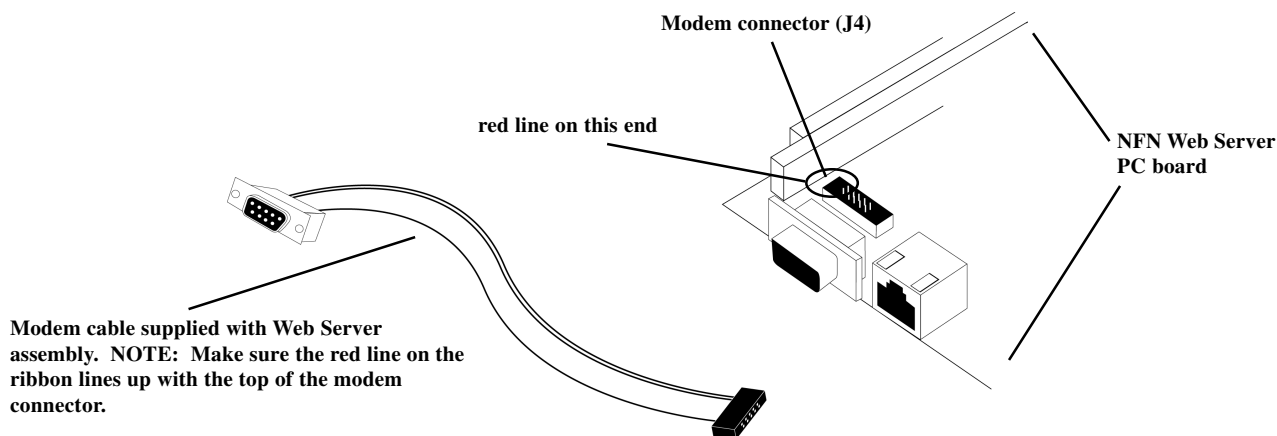


Figure 2.7-1: 10-Pin to DB-9 Connection (Modem Connection)

2.8 ETHERNET NETWORK CONNECTION

This connects the NFN Web Server to the Internet or Intranet. A PNET-1 surge suppressor must be used between the Web Server PC board and the network. Using the RJ45 cable, plug one end into the PC board and the other into the square end of the PNET-1. Then, connect another RJ45 cable from the PNET-1 out to the network.

The NFN Web Server can be used as a web-based gateway for communication between **NOTI•FIRE•NET™** and Veri•Fire™ Tools. The Ethernet port on the Web Server computer connects to the Ethernet port on the Veri•Fire™ Tools computer. For details on using Veri•Fire™ Tools with the NFN Web Server, consult the Veri•Fire™ Tools online help.

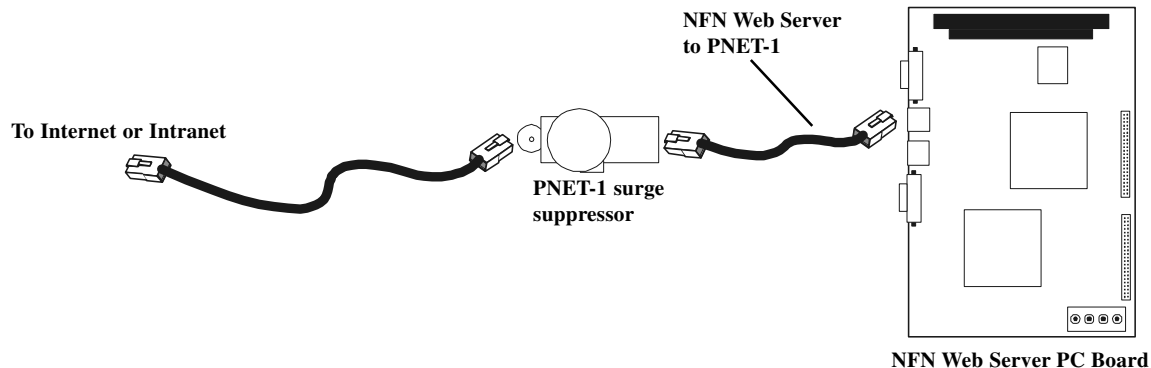


Figure 2.8-1: Ethernet Connection

2.9 PC TO PC CONNECTION

This connects the NFN Web Server to a PC that has one of the following programming utilities installed on it:

- Serial Configuration Tool (P/N NWS-SW)
- Veri•Fire™ Tools (P/N VERIFIRE-TCD)

This connection is used when configuring the Web Server.

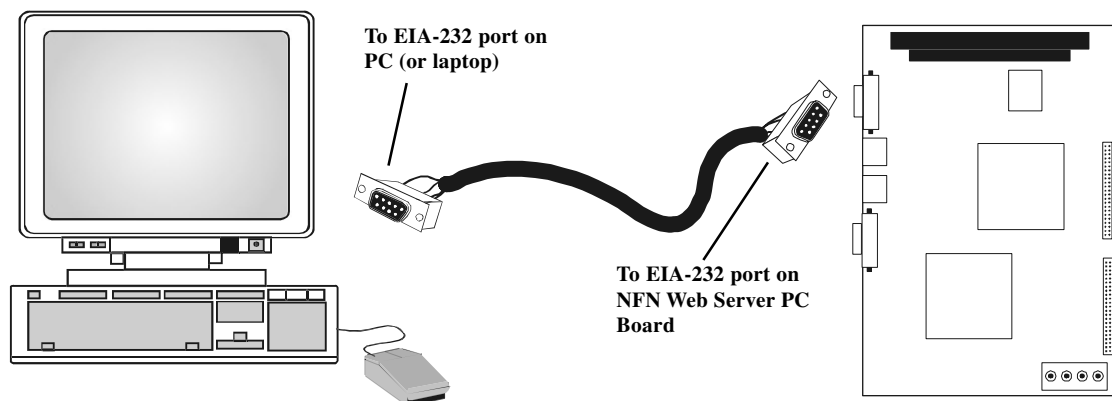


Figure 2.9-1: PC to PC Serial Connection



NOTES: Cable must be supplied by customer and must be a null-modem cable.

NOTES

SECTION THREE: NFN WEB SERVER CONFIGURATION

3.1 NFN WEB SERVER SERIAL CONFIGURATION TOOL INSTALLATION

There are two ways to configure the NFN Web Server: use the NWS configuration tool supplied on CD-ROM, or use Veri•Fire™ Tools, the **NOTI•FIRE•NET™** programming utility.

The Serial Configuration Tool software is supplied on CD-ROM. To install the application onto the PC or laptop, follow these steps:

1. Insert the CD-ROM into the CD-ROM drive.
2. If the CD does not automatically run the installation setup, from Windows Explorer or the Run command, execute setup.exe from the root directory of the CD-ROM.
3. This will execute the install application. Simply follow the directions on screen to install the Serial Configuration Tool.
4. Once it is installed, it can be launched from the Start menu by selecting Programs, VerFire Tools, NWS Configuration Tool.

3.2 USING THE NWS CONFIGURATION TOOL FOR CONFIGURATION

The NWS Configuration Tool configures network parameters of the Web Server. When you run the Configuration Tool, the following dialog box will be displayed:

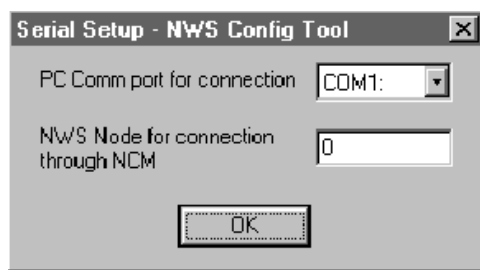


Figure 3.2-1: NFN Web Server Serial Setup Dialog

The Configuration Tool communicates with the Web Server either directly by connecting the PC to the server's serial port, or by connecting the PC to the second NUP port of an NCM that is on the same network as the Web Server. Note that if connected via an NCM, there must also be some type of node connected to the NCM which has caused the NCM to join the network. Enter the communications port that the PC is using for its connection to the Web Server. When connecting through an NCM, the Web Server node must be specified in the window above so the configuration tool can find it. When connecting directly, the node may be left as zero.

PC DIRECTLY CONNECTED TO NFN WEB SERVER

1. Select the COM port being used.
2. Click **OK** to finish configuration.

PC COMMUNICATING TO NFN WEB SERVER VIA NCM

***NOTE:** THIS OPTION IS ONLY USED WHEN IT IS NECESSARY TO RE-CONFIGURE THE WEB SERVER SETTINGS.

1. Select the COM port being used.
2. Specify the node number being used for the NFN Web Server.
3. Click **OK** to finish configuration.

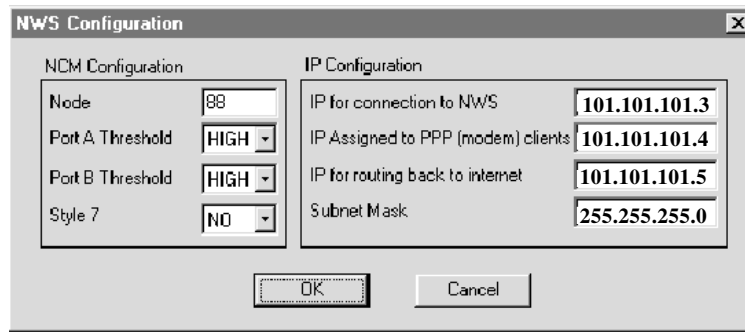
If the NFN Web Server does not yet have a node number, the PC must be connected directly to the Web Server first to give it one.



NOTE: To configure the NWS via an NCM, you must have a NUP-to-DB9 cable (P/N 75554).

After selecting **OK**, the configuration tool will attempt to communicate with the Web Server. In the case where communications can be established, it may take up to 10 seconds to finish the initial communications; however, if communications can not be established (because nothing is connected to the serial port), it will take up to 30 seconds before the Configuration Tool displays an error message.

After communication has been established, the following window will appear:



The image shows a dialog box titled "NWS Configuration". It is divided into two main sections: "NCM Configuration" and "IP Configuration".

NCM Configuration:

- Node: 88
- Port A Threshold: HIGH
- Port B Threshold: HIGH
- Style 7: NO

IP Configuration:

- IP for connection to NWS: 101.101.101.3
- IP Assigned to PPP (modem) clients: 101.101.101.4
- IP for routing back to internet: 101.101.101.5
- Subnet Mask: 255.255.255.0

At the bottom of the dialog box are two buttons: "OK" and "Cancel".

Figure 3.2-2: NFN Web Server Configuration

There are eight settings pertaining to the network setup of the Web Server; four of these pertain to parameters for use in establishing a **NOTI•FIRE•NET™** communications link through an NCM, and four of these pertain to allowing a browser to establish a connection.

NCM CONFIGURATION

The **Node** field is the node number you will use in connecting to **NOTI•FIRE•NET™**. If the configuration tool is connected through an NCM, the node number may not be changed; to change the node number, exit the configuration tool by pressing **Cancel**, then connect the PC directly to the Web Server and run the service tool again.

The threshold and style 7 settings are standard NCM settings; refer to the NCM documentation for an explanation of these fields.

IP CONFIGURATION

These four settings configure various IP parameters for use in connecting a browser.

IP FOR CONNECTION TO NWS sets the actual IP address where the Web Server will be located. The user will type this address into a browser in order to establish a connection with the Web Server. Note that if the Web Server is to be used on the internet, you may need to independently set up a router and/or firewall so the internet-based applications can locate and access the Web Server. Contact your MIS department for details. To actually connect to the Web Server requires use of TCP/IP port 8888; for example, if the NWS is located at 10.4.2.1, one would type:

<http://10.4.2.1:8888/>

into the browser window to connect to the Web Server.

IP ASSIGNED TO PPP (modem) CLIENTS sets the IP that the Web Server will assign to a computer when that computer attempts to connect to the Web Server over the modem connection. The Web Server acts as a PPP server with regard to a client computer on the modem connection, and one of its responsibilities is to assign the client's IP for purposes of the given modem session. This parameter is optional; if it is not intended that a browser be used to establish communications via a modem, it can be omitted.

IP FOR ROUTING BACK TO INTERNET sets the IP of a router that the Web Server can use to locate the browser with which it is communicating. This simply sets a path for the Web Server to use to communicate back with the connecting browser.

SUBNET MASK is the IP subnet mask that the Web Server should use to determine whether a connection came from a local network, or should be routed on to another network (see previous setting). All of the IP settings for the Web Server must be on the same subnet for communications to be established between the Web Server and a browser.



IMPORTANT: When making an update to the Web Server software, from the Internet Explorer browser you must select *Tools, Internet Options*, then click on the *Delete Files* button, check *Delete all offline content*, then click *OK* to finish the process.

3.3 USING VERI•FIRE™ TOOLS FOR CONFIGURATION

Veri•Fire™ Tools is supplied on CD-ROM. To install the application onto the PC or laptop, follow these steps:

1. Insert the CD-ROM into the CD-ROM drive.
2. From Windows Explorer or the Run command, execute setup.exe from the root directory of the CD-ROM.
3. This will execute the install application. Follow the directions on screen to install Veri•Fire™ Tools.
4. Once it is installed, it can be launched from the Start menu by selecting **Programs, VeriFire Tools, VeriFire Tools**.



NOTE: The NFN Web Server is compatible with Veri•Fire™ Tools version 3.00 or later.

Veri•Fire™ Tools can communicate with the Web Server in one of two ways:

1. Direct communication by connecting Veri•Fire's PC to the web server's serial port - this connection, using DB9-DB9, is used for the Web Server's initial setup to be able to communicate over the NFN network.
2. Communication over the NFN network by connecting Veri•Fire's PC to the second NUP port of an NCM that is on the same network as the Web Server.

THE SERIAL PORT CONFIGURATION UTILITY

To activate communications between the PC and the NFN Web Server, use the Serial Port Configuration Utility, accessed from the Start menu by selecting **Start, Programs, VeriFire Tools, Serial Port Configuration Utility**. The NUP Serial Port Auto Configuration dialog will appear (seen in Figure 3.3-1).

PC DIRECTLY CONNECTED TO NFN WEB SERVER

For a PC directly connected to the NFN Web Server, click on the **Auto Configuration** button to establish communications. When finished, exit by clicking on the **x** button in the top right corner.

IMPORTANT: *When the NFN Web Server is first being configured, you must use this direct serial connection to initially establish communication between the Web Server and the PC.*

PC COMMUNICATING TO NFN WEB SERVER VIA NCM

NOTE: THIS OPTION IS ONLY USED WHEN IT IS NECESSARY TO RE-CONFIGURE THE WEB SERVER SETTINGS.

For a PC Communicating to NFN Web Server Via the NCM, run the Serial Port Configuration Utility to establish communications.

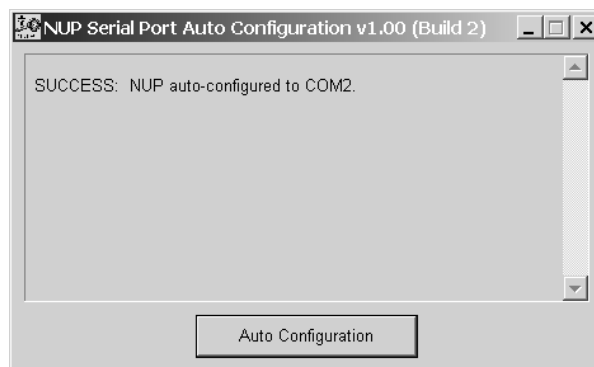


Figure 3.3-1: Serial Port Configuration Utility



NOTES: If the Web Server is to be connected via an NCM, you must specify the node number being used for the NFN Web Server by accessing Veri•Fire™ Tools.

If the NFN Web Server does not yet have a node number, the PC must be connected directly to the Web Server first to give it one.



NOTE: To configure the NWS via an NCM, you must have a NUP-to-DB9 cable (P/N 75554, sold separately).

3.4 INITIAL SETUP OF THE NFN WEB SERVER

1. Make a PC-to-PC hardware connection between Veri•Fire™ and the NFN Web Server (see Figure 2.9-1).
2. Open Veri•Fire™ by selecting **Start, Programs, VeriFire Tools, VeriFire Tools**.
3. Select **Local** from the Connection Type area of the screen, then click **OK**.

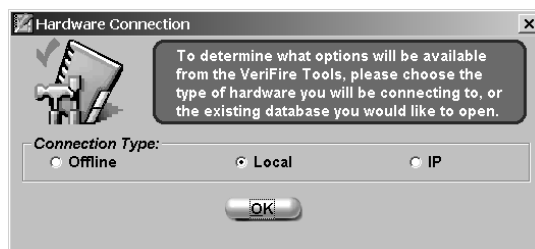


Figure 3.4-1: Veri•Fire™ Local Connection Type

4. Next, double click on the NFN Web Server entry on the Nodes screen. This will bring up the main configuration screen that will be used to set up the NFN Web Server for communication over the network.

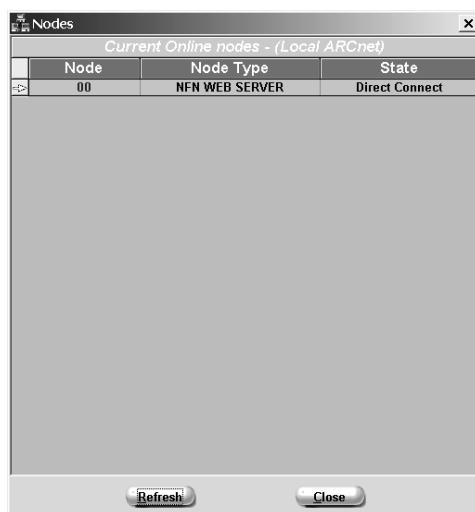
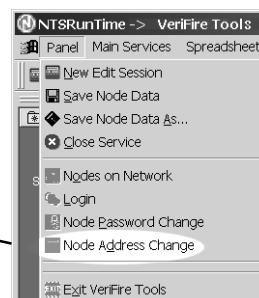
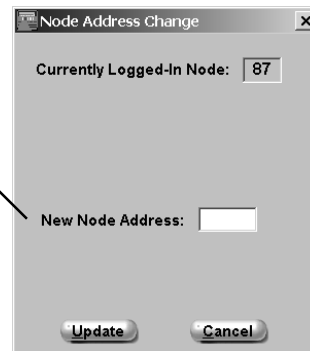


Figure 3.4-2: Nodes Screen

5. Before making Web Server configuration settings, assign the Web Server a unique NFN node address. From the Veri•Fire™ menu bar, select **Panel, Node Address Change**.



6. Type in the node address, and click **Update** to apply the changes.



The Web Server can now be configured for communication over **NOTI•FIRE•NET™**.

The following fields must be configured to run the NFN Web Server:

IP address for connection to Notifier - This is the actual IP address where the Web Server will be located. Type the address by double clicking on the data field to the right of the description field. The user will type this address into a browser in order to establish a connection with the Web Server. If the Web Server is to be used on the internet, you may need to independently set up a router and/or firewall so the internet-based applications can locate and access the Web Server. Contact your MIS department for details. To actually connect to the Web Server requires use of TCP/IP port 8888; for example, if the NWS is located at 10.4.2.1, one would type the following into the browser window to connect to the Web Server.:

<http://10.4.2.1:8888/>



NOTE: Fields marked with an asterisk are editable within their respective data fields.

The screenshot shows the 'Read Status Service' window in VeriFire Tools. The window has a menu bar (Panel, Main Services, Spreadsheets, Reports, View, Utilities, Network Diagnostics, Documents, Help) and a toolbar. On the left is a sidebar with 'Main Services' (Read Status, Upload/Download) and a list of other services (Spreadsheets, Reports, View, Utilities, Network Diag. Serv., Documentation). The main area is titled 'Read Status Service' and includes a 'Current Network Node Address' field set to '87' and a 'Close' button. Below this is a table of configuration settings for 'NFN Web Server Node 87'. The table has two columns: 'Description Field' and 'Data Field'. Fields marked with an asterisk (*) are editable. A callout box points to the 'Drop number' field (87) with the text 'This is the node number.' At the bottom of the window are 'Program' and 'Refresh' buttons. The Windows taskbar at the bottom shows the Start button, open files (NTSRunTime.md..., untitled - Paint), and the system clock (9:44 AM).

Description Field	Data Field
* IP address for connection to Notifier	101.101.101.101
* Subnet mask	255.255.255.0
* IP address for routing back to Internet	101.101.101.1
Primary port	0
Secondary port	0
* IP address assigned to PPP(modem)	0.0.0.0
Network number	0
Drop number	87
Port number	0
* NCM Thresholds	Port A High, Port B High
* Network Style	Style 4

Figure 3.4-3: NFN Web Server Configuration Settings

Subnet Mask - This is the IP subnet mask that the Web Server should use to determine whether a connection came from a local network, or should be routed on to another network (see previous setting). All of the IP settings for the Web Server must be on the same subnet for communications to be established between the Web Server and a browser.

IP address for routing back to Internet - This sets the IP of a router that the Web Server can use to locate the browser with which it is communicating. This simply sets a path for the Web Server to use to communicate back with the connecting browser.

IP address assigned to PPP (modem) - This sets the IP that the Web Server will assign to a computer when that computer attempts to connect to the Web Server over the modem connection. The Web Server acts as a PPP server with regard to a client computer on the modem connection, and one of its responsibilities is to assign the client's IP for purposes of the given modem session. This parameter is optional; if it is not intended that a browser be used to establish communications via a modem, it can be omitted.

NCM Threshold and Network Styles - The NCM threshold can be set to high or low, and the network style can be set to style 4 or style 7. Refer to the NCM documentation for more details on these fields.

LAUNCHING VERIFIRE™ TOOLS

This section describes how to access NFN Web Server configuration information using Veri•Fire™ Tools.

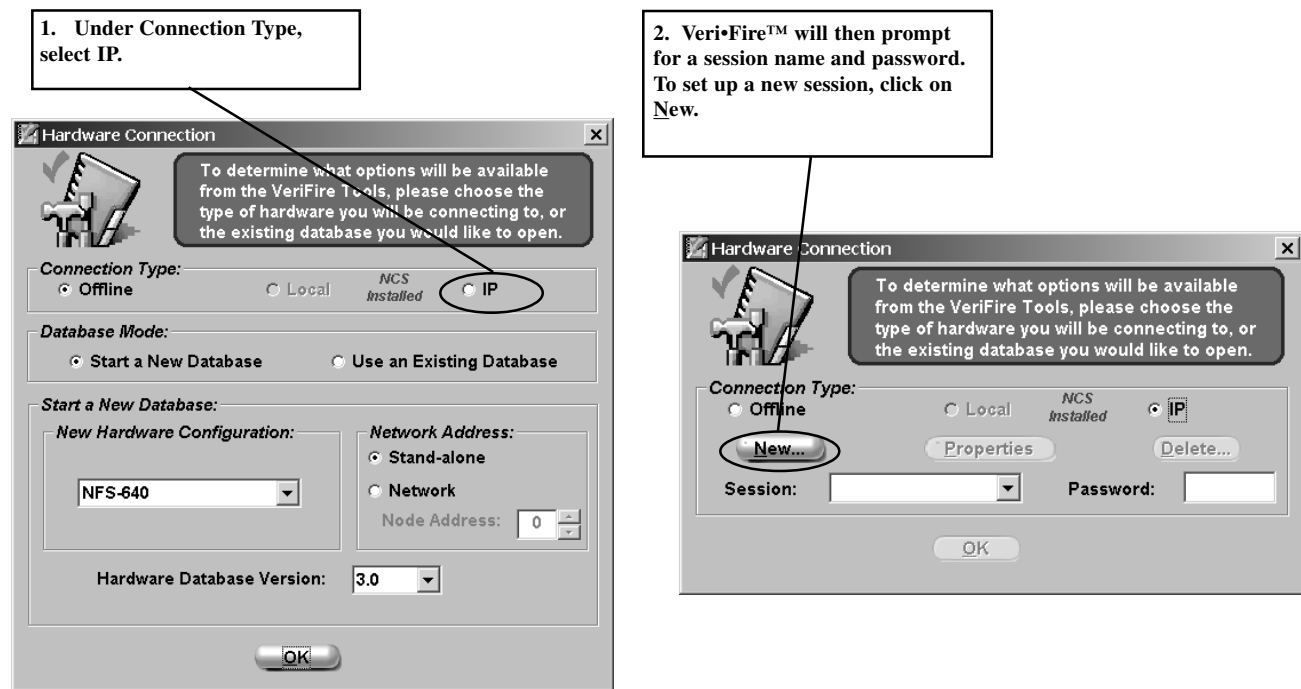


Figure 3.4-4: Selecting the Connection Type

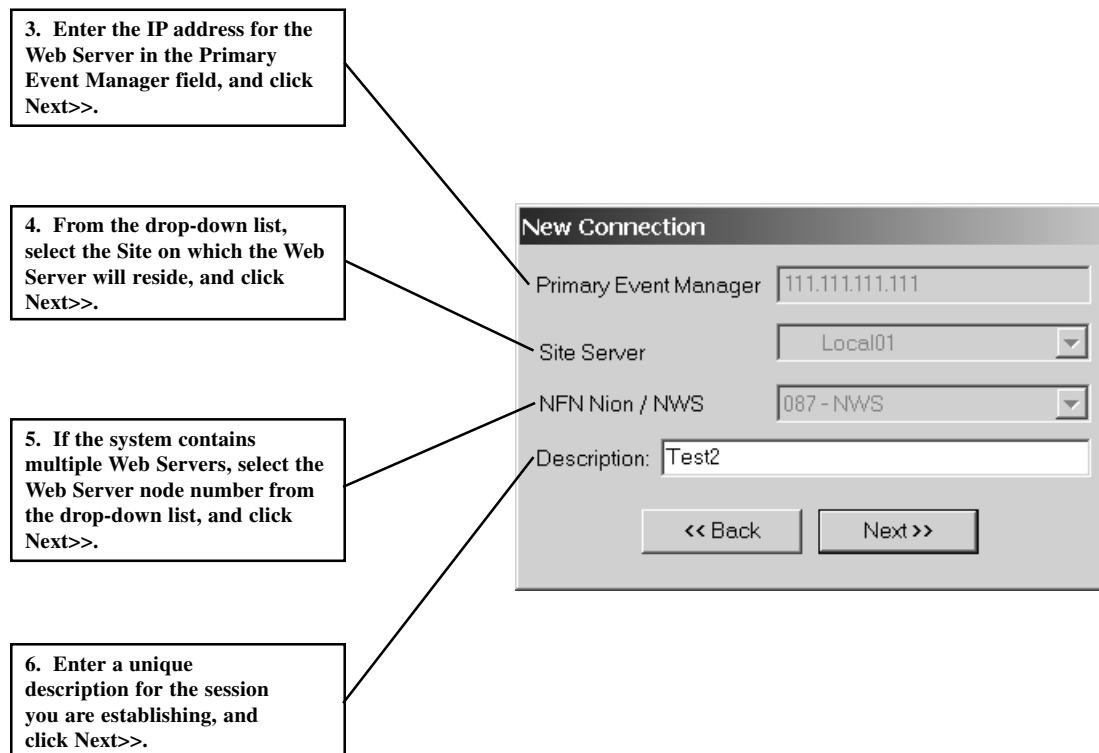


Figure 3.4-5: Configuring the Web Server Connection Session

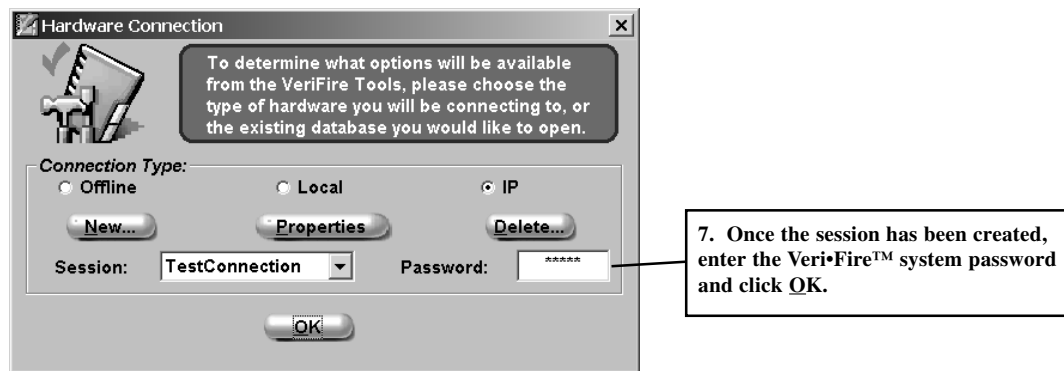


Figure 3.4-6: Veri•Fire™ Tools System Password

Once you are online, VeriFire™ Tools will prompt you to select the Hardware Connection, which will be NFN Web Server, as seen in Figure 3.4-7. Double click on it to proceed to the configuration screen.

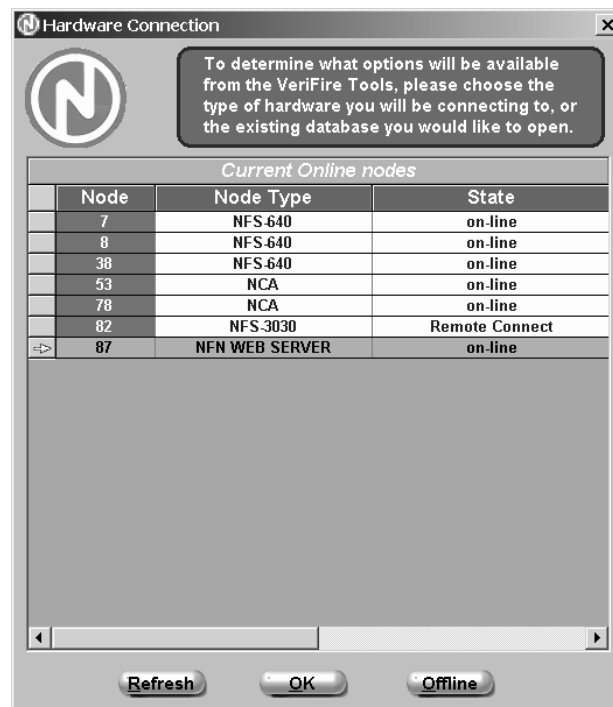


Figure 3.4-7: Selecting the Connection Type

CHANGING THE NODE NUMBER

The Node Number (or Drop Number as displayed on the previous screen) is the node address of the NFN Web Server. To change this number using Veri•Fire™ Tools, select **Panel, Node Address Change** from the menu bar on the main screen.

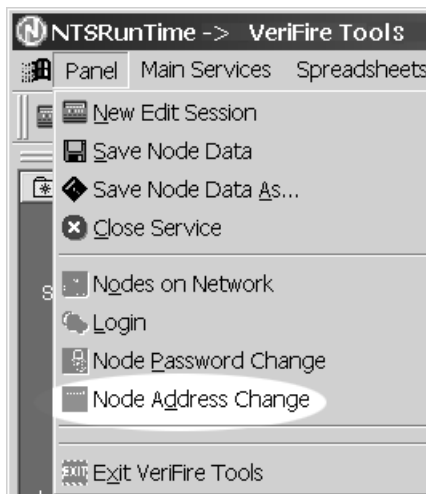


Figure 3.4-8: Changing the Node Address

Type in the new node address, and click **Update** to apply the changes, or **Cancel** to exit without changing the address.

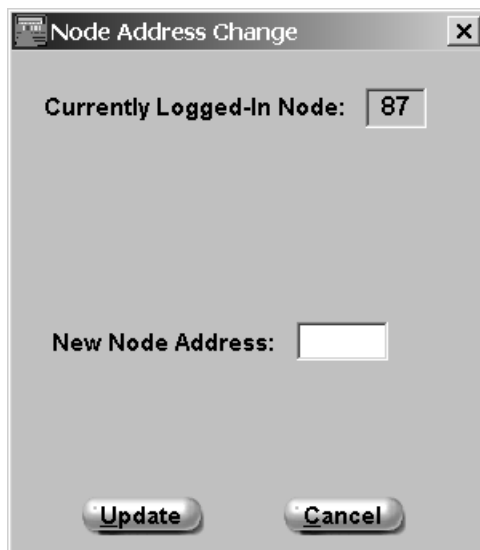


Figure 3.4-9: Changing the Node Address

SECTION FOUR: NFN WEB SERVER OPERATION

4.1 NFN WEB SERVER SECURITY

The user default ID is “users,” and the user default password is “11111.” The Admin default ID is “admin,” and the admin default password is “00000.” These passwords should be modified as soon as possible to retain system security.

When the application is started, a user or administrator must log in to have access to functions assigned to him/her by the system administrator. To log in, enter your User ID and password, then click **OK**.

You can choose to **Save this password in your password list**; this option will automatically fill in the password for the chosen User Name on the current PC.



NOTE: Passwords are case sensitive.



Figure 4.1-1: NFN Web Server Login Dialog

4.2 THE BROWSER INTERFACE

The NFN Web Browser Interface displays information about all points present and active on **NOTI•FIRE•NET™**. The browser is the standard Microsoft Internet Explorer format. For details on navigating Microsoft Internet Explorer, consult its corresponding documentation or help file.

The display screen is divided into two sections: on the left-hand side is an Explorer-style collapsible/expandable tree to choose specific nodes and browser configuration menu items. The right area of the screen displays the chosen option, such as properties for a device on a specific node, or configuration setting fields for a selected configuration option.

The NWS Home Page link navigates to the main screen (shown in this example).

The link below the NWS Home Page link navigates to the custom defined URL configured in System Settings.

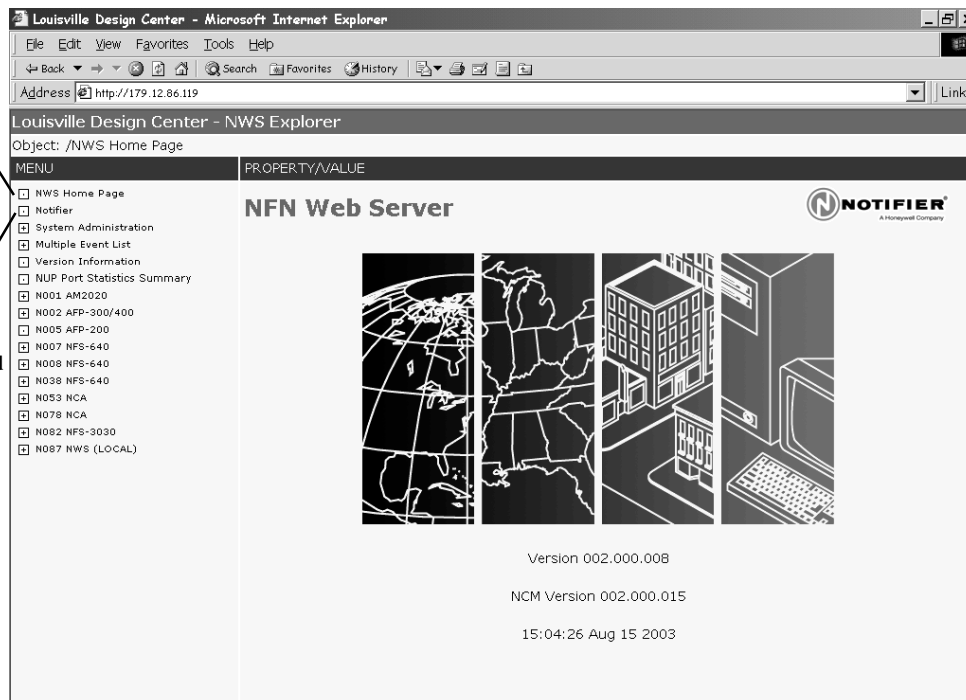


Figure 4.2-1: NWS Home Page

4.3 SYSTEM ADMINISTRATION

The System Administration setup options configure various NFN Web Server settings and can only be accessed by administrator level operators.

4.3.1 AUTO DETECT POINTS ON ALL PANELS

This option will auto detect AFP1010/AM2020 points on **NOTI•FIRE•NET™**.

How Points Become Visible To The Web Server

There are three ways a point becomes visible to the Web Server:

1. With Onyx series panels, points are detected automatically when the Web Server is connected to the network on which those panels reside. Therefore, point detection for ONYX series panels requires no user action.
2. With AFP1010/AM2020 panels, points are only detected when a user clicks on the AutoDetect menu item either under the individual AFP1010/AM2020 panel's menu, or under System Administration. Although the feature is called Auto Detect, this requires the user action of clicking on the Auto Detect command.
3. With AFP-300/400 panels, points are only detected when they generate an event, which can then be seen by the Web Server; therefore, the only way to add points connected to an AFP-300/400 panel is to manually generate an event for each point.

Events from points that have not been Auto Detected will be shown in the Multiple Events list. In other words, events coming from a classic panel will be logged even if the points themselves did not previously appear in the hierarchy list at the left of the NWS screen.

A Note On AFP-200 Panel Points

AFP-200 points do not get Auto Detected, and they will not be displayed in the hierarchy list on the left. However, events from an AFP-200 panel and/or point will come into the Multiple Event List and can generate an email.

Selecting this option will navigate to the corresponding screen at the right, the Auto Point Detect Verification screen. This screen requests that the administrator verify the auto discover command, as the process can be time-consuming, depending on the size of the entire system.



NOTE: Only administrators have security access to the auto detect feature.

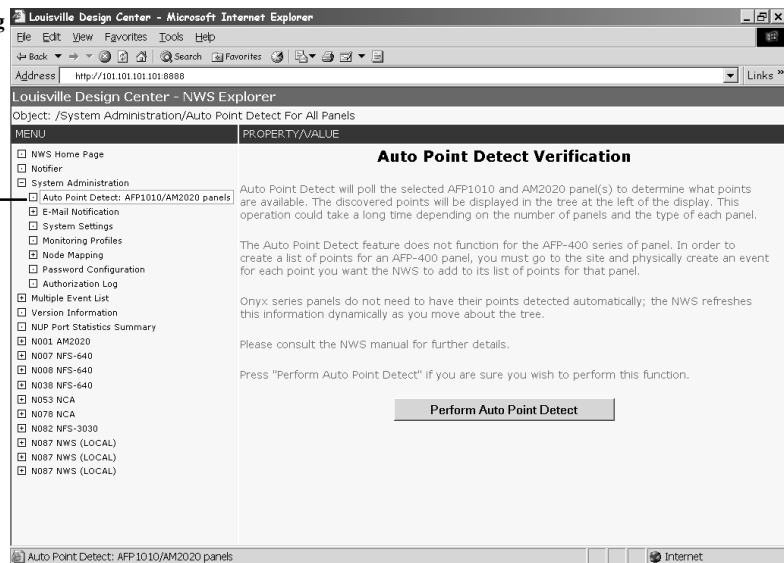


Figure 4.3.1-1: Auto Detect Points

The Auto Point Detect feature does not function for the AFP-300/400 panel, as seen on the screen message shown below.

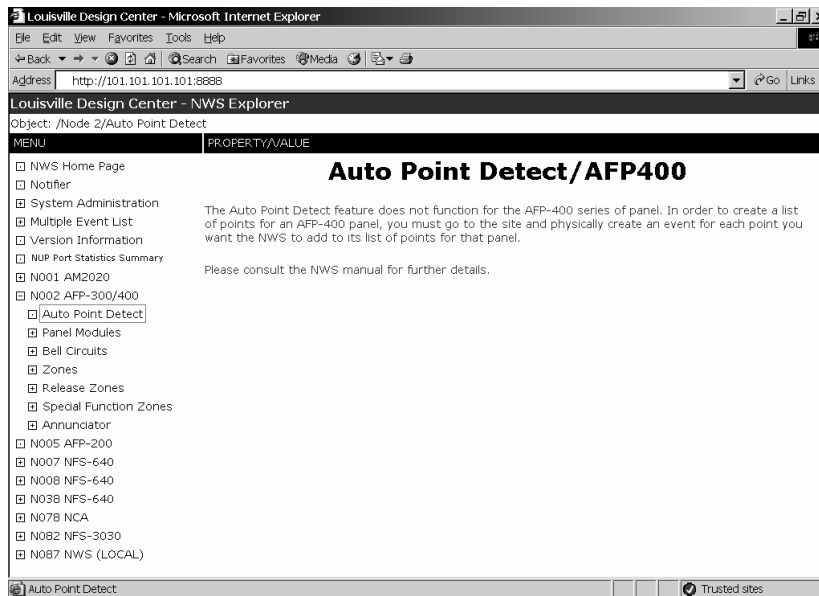
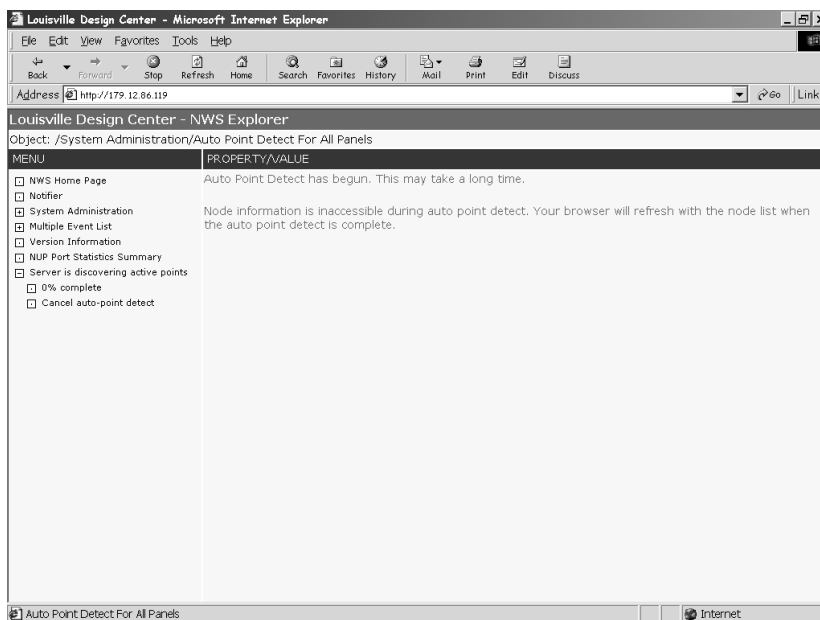


Figure 4.3.1-2: Auto Point Detect AFP400 Message



This lets you know that the Auto Detect task is currently being performed.

This line denotes the current progress of the Auto Detect task.

This option allows you to cancel out of Auto Detect if necessary.

Figure 4.3.1-3: Auto Detect Screen

Once the Auto Detect has been performed, go to the Node Mapping links and make sure that all node numbers that read "online" are also mapped. Refer to section 4.3.4 Node Mapping for more information.

4.3.2 E-MAIL NOTIFICATION

SUMMARY

The e-mail notification feature enables the administrator to configure the NWS to automatically send event information via e-mail to a select group of users. E-mail recipients receive events according to the profiles they have been assigned. The NWS can support a maximum of ten profiles, and an e-mail recipient can be assigned to all ten profiles. Each of the ten profiles support a maximum of five e-mail addresses.

E-MAIL CONFIGURATION

You will need the following information from your Internet Service Provider (ISP) or Local Area Network (LAN) administrator. The NWS does not provide authentication information.

Outgoing Mail IP Address (SMTP) - This is the mail server's IP address. The NWS does not support DNS; therefore, you will need the address in dotted decimal form (XXX.XXX.XXX.XXX).

Mail User - This is an SMTP server setting. Leave this field blank unless your network administrator indicates otherwise.

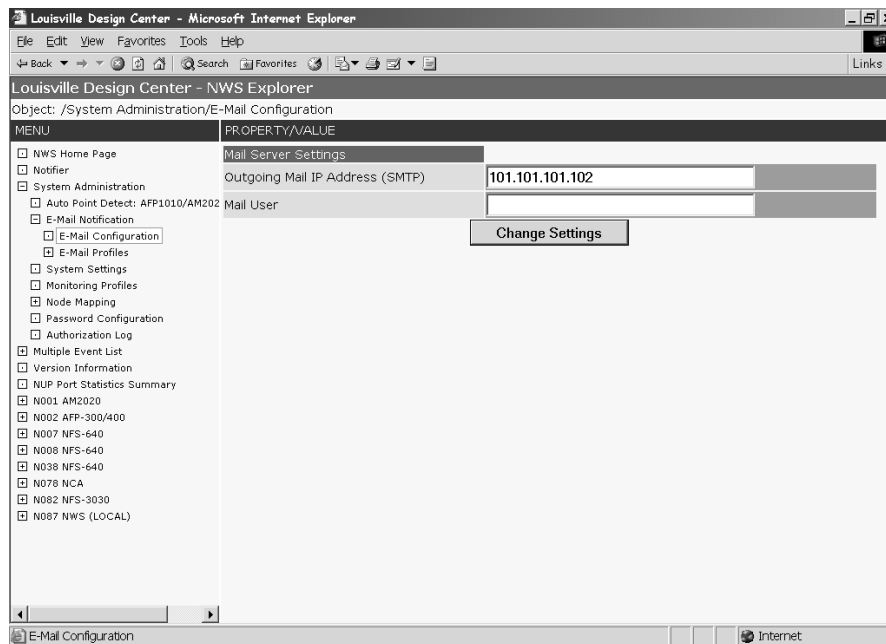


Figure 4.3.2-1: E-mail Configuration

E-MAIL NOTIFICATION FEATURES

The following lists some of the benefits that the e-mail notification feature provides:

- Ten Profiles
- Send up to 50 e-mails in response to any system event
- Quickly Enable and Disable E-mail feature
- Create your own custom messages that will be included with the e-mailed system event

CONFIGURING E-MAIL PROFILES

Profiles define the e-mail addresses of the recipients assigned that profile, along with the nodes and event types that will initiate an e-mail message. Profiles filter e-mail notification by event type. The six event types are Fire Alarms, Pre-Alarms, Securities, Supervisories, Troubles, and Other.

To access E-mail Profiles, from the menu hierarchy on the left, click on System Administration, then click on E-mail Profiles to expand the selection to display the ten profiles.

1. Select the profile to define from the list on the left.
2. Enter the e-mail addresses to be included in the profile for notification.
3. Choose the node (panel type) to be included for email notification.
4. Choose the event types to be included for email notification. Note that these are set on a per-node basis.
5. Configure custom messages (see Figure 4.3.2-3).
5. After making all settings for the profile, click on **Save Profile** to apply the settings.

Disable Profile - By checking the **Disable Profile** option, this will prevent e-mails from being sent for this profile until the box is un-checked. Profiles are enabled by default.

Each profile can define up to ten nodes that will be included in e-mail notification. This includes an "all nodes" setting as well.

Each profile can define up to five e-mail addresses to which the profile will apply.

E-Mail Profile #1

Object: /System Administration/E-Mail Profiles/profile 1

MENU: PROPERTY/VALUE

System Administration
Auto Point Detect For A
E-Mail Notification
E-Mail Configuration
E-Mail Profiles
Profile 1
Profile 2
Profile 3
Profile 4
Profile 5
Profile 6
Profile 7
Profile 8
Profile 9
Profile 10
System Settings
Monitoring Profiles
Node Mapping
Password Configuration
Authorization Log
Multiple Event List
Version Information
NUP Port Statistics Sumr
N001 AM2020
N007 NFS-640
N008 NFS-640
N038 NFS-640

Disable Profile ☐

Save Profile

Node	Fire Alarm	Pre-Alarm	Trouble	Security	Supervisory	Disabled	Other
N001 AM2020	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
N007 NFS-640	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
N082 NFS-3030	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
N087 NWS	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
None	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
None	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
None	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

E-Mail addresses

email1@yourdomain.com
email2@yourdomain.com
email3@yourdomain.com
email4@yourdomain.com
email5@yourdomain.com

Profile 1

Internet

Figure 4.3.2-2: E-mail Profile Configuration

CUSTOM MESSAGES

The administrator can define a 50-character max. custom message corresponding to the event types. These messages will be included in the body of any e-mails sent to specified recipients.

Custom messages are defined according to event type and have a 50-character maximum.

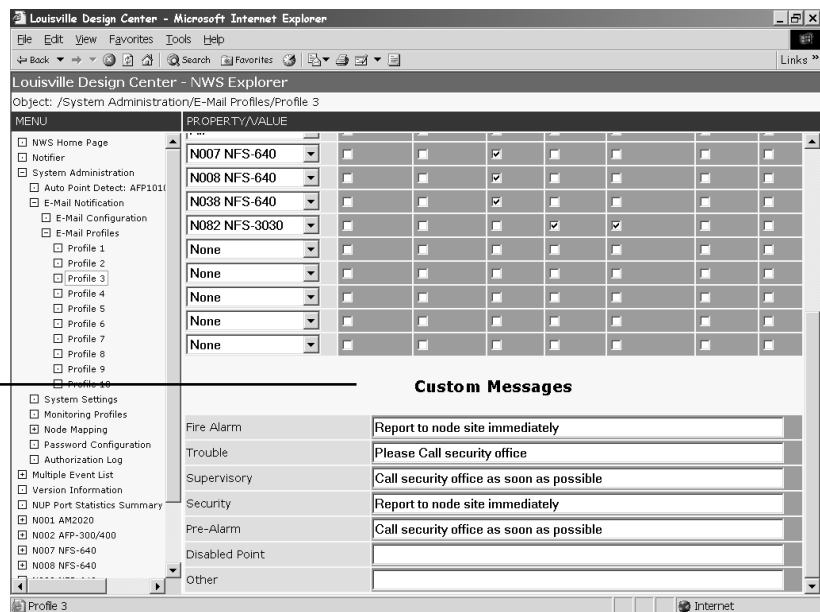


Figure 4.3.2-3: Email Configuration - Custom Messages

In the example illustrated in Figure 4.3.2-3 above, custom messages have been defined for various event types. Above the Custom Messages area, NCA nodes can be configured for email notification according to various event types. The general appearance of the email notification message will vary depending on the email application used, individual PC font settings, and other factors. A sample message, however, can be seen in Figure 4.3.2-4.

The Site Name denotes where the NWS is located. The Site Name is configurable under System Administration, System Settings.

The information under Event displays detailed event information in the same format as that of the panel or annunciator.

This is the custom message that was defined for this event type.

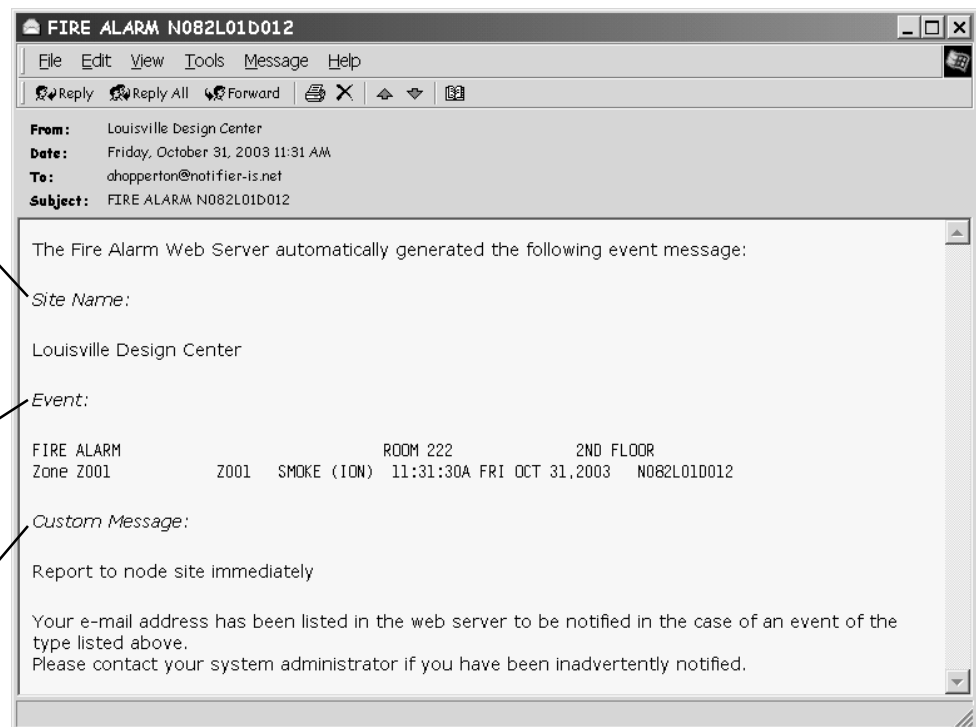


Figure 4.3.2-4: Sample Email Message

4.3.3 SYSTEM SETTINGS

Selecting System Administration, System Settings allows you to make NFN Web Server browser configuration settings.

The screenshot shows a web browser window titled "Louisville Design Center - Microsoft Internet Explorer". The address bar shows "http://179.12.86.119". The page content is titled "Louisville Design Center - NWS Explorer" and "Object: /System Administration/System Settings".

MENU

- ☐ NWS Home Page
- ☐ Notifier
- ☐ System Administration
 - ☐ Auto Point Detect For All Panels
 - ☐ E-Mail Notification
 - ☐ System Settings
 - ☐ Monitoring Profiles
 - ☐ Node Mapping
 - ☐ Password Configuration
 - ☐ Authorization Log
- ☐ Multiple Event List
- ☐ Version Information
- ☐ NUP Port Statistics Summary
 - ☐ N001 AM2020
 - ☐ N002 AFP-300/400
 - ☐ N005 AFP-200
 - ☐ N007 NFS-640
 - ☐ N008 NFS-640
 - ☐ N038 NFS-640
 - ☐ N053 NCA
 - ☐ N078 NCA
 - ☐ N082 NFS-3030
 - ☐ N087 NWS (LOCAL)

PROPERTY/VALUE

Site Settings	
Site Name	Louisville Design Center
Site Link	http://www.notifier.com
Site Link Name	Notifier
General Settings	
Non-Admin User Access	Enabled
Network Update	No
Network Update Time (hh:mm)	21:32
Trouble Reminder	Yes
Event Refresh Time (0, or 3-90 seconds)	5
Unacknowledged Beep	<input type="checkbox"/>
NCM Settings	
Node Address	87
Channel A Threshold	high
Channel B Threshold	high
Style 7	No

Change Settings

Figure 4.3.3-1 System Settings

SITE SETTINGS

Site Name - This is a user defined field designed to facilitate a unique descriptive name for the NFN Web Browser.

Site Link - This is a user defined field that allows you to add a shortcut to the link list at the left of the NFN Web Browser window. This link can be to a graphic image of the network site or a company homepage.

Site Link Name - This is the name that will be displayed in the browser header when the Site Link address is accessed.



NOTE: Only alphanumeric characters are supported for the Site Settings fields, with the exception of the colon, forward slash and period.

GENERAL SETTINGS

Non-Admin User Access - This setting defines whether or not operators will have access to the NFN Web Server.

Network Update - Select **Yes** to have the NFN Web Server auto detect points daily.

Network Update Time - If the Web Server is configured to auto detect points daily, this field is used to select the time you want the Web Server to perform this action.

Trouble Reminder - If there is an active trouble on the network, every 24 hours at 11:00 AM, a trouble reminder message will be generated across the network.

Event Refresh Time - This field is used to specify a refresh rate (between 3 and 90 seconds) for the Multiple Event List. The NWS will automatically refresh itself at the specified interval. Any new system event will be displayed in the Multiple Event List. To disable this feature, set the time to 0.

Unacknowledged Beep - Check this option to enable an audible reminder of unacknowledged events. When this is checked, the Web Server will beep at 3-second intervals and will continue until no unacknowledged events are shown in the Multiple Events List.

NCM SETTINGS

Node Address - The node where the NCM is located on the **NOTI•FIRE•NET™** network.

Channel A/B Threshold - Threshold settings are used according to the amount of network noise present; changing the threshold settings will initialize the NCM board itself.

Style 7 - Select **Yes** if style 7 is being used.

4.3.4 MONITORING PROFILES

Selecting System Administration, Monitoring Profiles allows you to select the event types to be displayed in the NFN Web Browser. Select No to disable NFN Web Browser viewing of the specified event type. The default value for all event types is **Yes**.

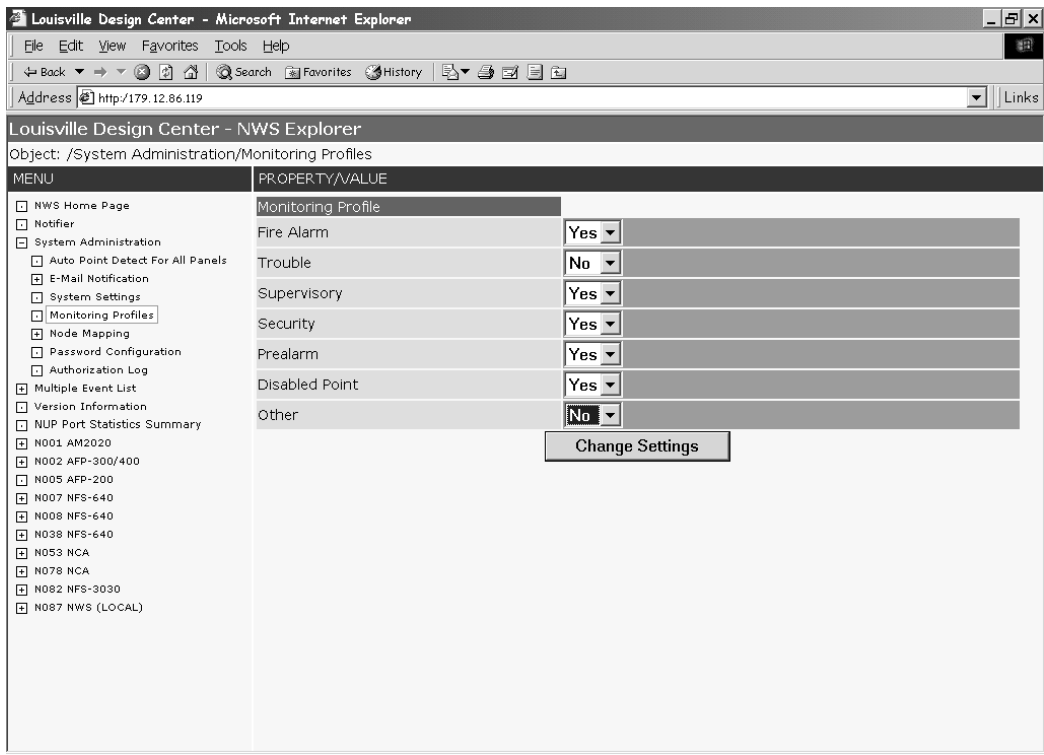


Figure 4.3.4-1: Monitoring Profiles

4.3.5 NODE MAPPING

Selecting System Administration, Node Mapping allows the user to map nodes that are active on the **NOTI•FIRE•NET™** network.

When the Auto Detect command is performed, the NFN Web Browser will determine whether a point (node) is online or offline. Then, you can use the Node Mapping links to view the results of the auto detection. For any node that is online, you must select Mapped for the NFN Web Browser to display events from that node, then click on the **Change Settings** button at the bottom of the web page.

The Auto Detect command located at the bottom of the screen will mark all online nodes as “mapped” and all offline nodes as “unmapped.”

If Unmapped, the NFN Web Browser will not display events from that node. You will not see events or properties from any new nodes until they are mapped from this page.



NOTE: The default value for node status is *Unmapped*.

Node Mapping Links

MENU	PROPERTY/VALUE
<input type="checkbox"/> NWS Home Page	Mapping Profile
<input type="checkbox"/> Notifier	Node 1 ONLINE Mapped
<input type="checkbox"/> System Administration	Node 2 OFFLINE Unmapped
<input type="checkbox"/> Auto Point Detect For All Pa	Node 3 OFFLINE Unmapped
<input type="checkbox"/> E-Mail Notification	Node 4 OFFLINE Unmapped
<input type="checkbox"/> System Settings	Node 5 OFFLINE Unmapped
<input type="checkbox"/> Monitoring Profiles	Node 6 OFFLINE Unmapped
<input type="checkbox"/> Node Mapping	Node 7 ONLINE Mapped
<input type="checkbox"/> Nodes 001-030	Node 8 ONLINE Mapped
<input type="checkbox"/> Nodes 031-060	Node 9 OFFLINE Unmapped
<input type="checkbox"/> Nodes 061-090	Node 10 OFFLINE Unmapped
<input type="checkbox"/> Nodes 091-120	Node 11 OFFLINE Unmapped
<input type="checkbox"/> Nodes 121-150	Node 12 OFFLINE Unmapped
<input type="checkbox"/> Nodes 151-180	Node 13 OFFLINE Unmapped
<input type="checkbox"/> Nodes 181-210	Node 14 OFFLINE Unmapped
<input type="checkbox"/> Nodes 211-240	Node 15 OFFLINE Unmapped
<input type="checkbox"/> Password Configuration	Node 16 OFFLINE Unmapped
<input type="checkbox"/> Authorization Log	Node 17 OFFLINE Unmapped
<input type="checkbox"/> Multiple Event List	Node 18 OFFLINE Unmapped
<input type="checkbox"/> Version Information	
<input type="checkbox"/> NUP Port Statistics Summary	
<input type="checkbox"/> N001 AM2020	
<input type="checkbox"/> N007 NFS-640	
<input type="checkbox"/> N008 NFS-640	
<input type="checkbox"/> N038 NFS-640	
<input type="checkbox"/> N082 NFS-3030	

Figure 4.3.5-1: Node Mapping

FOUR NODE STATUS VALUES:

1. **Online** - The node was auto detected by the NFN Web Browser, but it will not show up in the Menu at the left, nor will events be displayed, until it is mapped.
2. **Offline** - There is no device detected at that node address. No events will be reported.
3. **Mapped** - If the node is online, it will show up in the Menu, and events will be displayed in the browser.
4. **Unmapped** - The default value; the node is either online with no event reporting, or there is no device detected at that node address. No events or properties will be displayed for unmapped nodes.

4.3.6 PASSWORD CONFIGURATION

Selecting System Administration, Password Configuration allows you to create, modify and delete system users and their access profiles. The system will support up to 128 total IDs. The page includes brief instructions on how to set up admin and user profiles. The username must be between 3 and 15 characters. The password must be between 5 and 8 characters.



NOTE: Users cannot access the System Administration menu. Only administrators have access to this configuration function.

IMPORTANT: To ensure system security, when finished with the Web Server, exit completely out of your internet browser.



NOTE: You must set up the Veri•Fire™ password first before setting up the user's NWS password and characteristics.

This is where users and their corresponding passwords are created.

Once a user has been created, his/her name is added to the drop-down selection box in the Characteristics section. This is where users are assigned access levels. Admin allows System Administration access, Verifire Read Status allows the user to access VeriFire for viewing point status information, and Verifire Control allows the user to access VeriFire for control and configuration functions.

How to add a user:

- type in a new User name and password
- retype password in "verify" field
- press the "Add" button

How to select characteristics:

- select User name
- press the "Refresh Characteristics" button
- change the characteristics
- press the "Change Characteristics" button

How to delete a user:

- select User name to delete
- press the "Delete" button

How to modify a user's password:

- select User name to modify
- type in a new password
- retype password in "verify" field
- press the "Modify Password" button

How to disable or enable a user:

- select User name to disable or enable
- press the "Disable/Enable" button
- disabled Users have a * next to their name

The interface includes form fields for Username, Password, Verify, Admin (dropdown), Verifire Read Status (checkbox), Verifire Control (checkbox), and buttons for Add Entry, Refresh Characteristics, Change Characteristics, Delete Entry, Modify Password, and Disable/Enable Entry.

Figure 4.3.6-1: User Configuration

4.3.7 AUTHORIZATION LOG

The Authorization Log displays a history of the last 50 users to access the NFN Web Server and includes the date and time of access. **IMPORTANT: The history does not include failed or denied accesses. The NWS does not keep a record of any failed attempts to access the web server.**

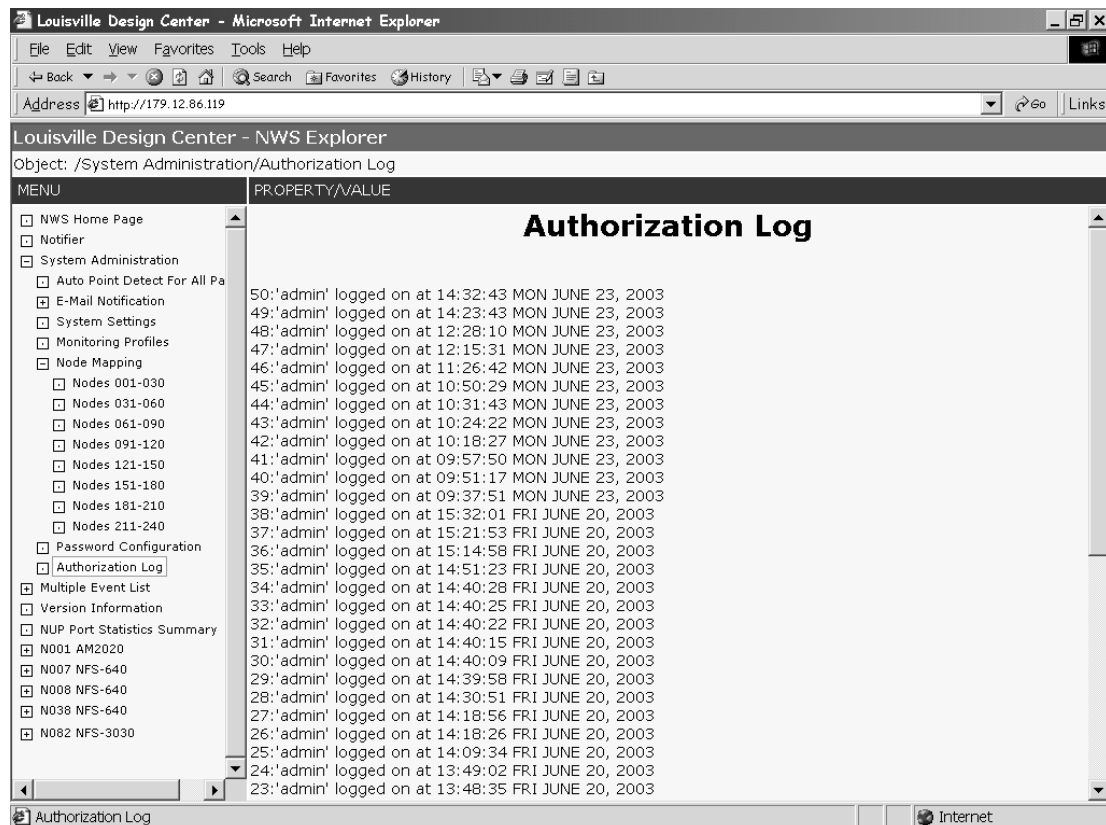


Figure 4.3.7-1: Authorization Log

4.4 MULTIPLE EVENT LIST

The Multiple Event List screen displays an event count, sorted by event type. Below is an example showing multiple Fire Alarms and Troubles. To view event details, click on a specific event type from the menu list.

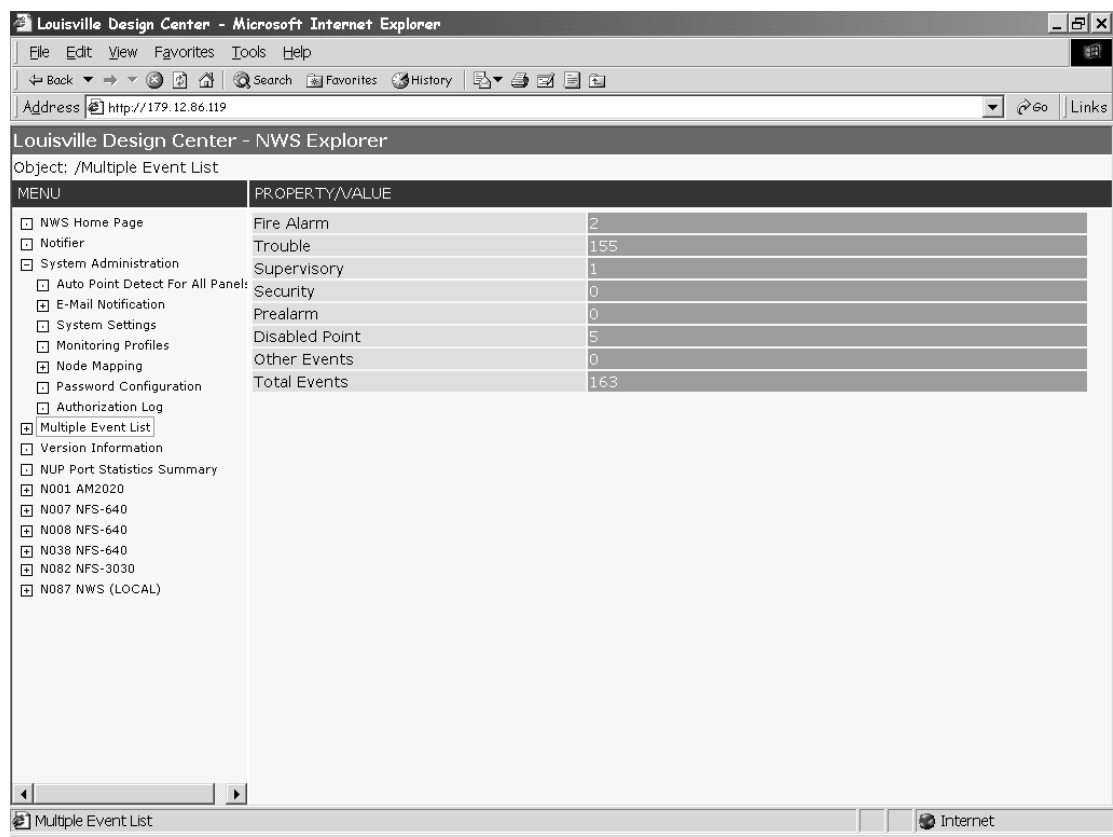


Figure 4.4-1: Event List Summary

Once an event type is selected, details are displayed on the resulting screen. If there are no events for a chosen event type, the screen will display a message saying “No events exist in this category.”



NOTE: The Web Server automatically extracts custom labels from panels when displaying events on an as-needed basis. When there are many classic panel events (i.e. AM2020/AFP1010), this process may take 30-40 seconds per page. The NWS will remember the extracted labels once it has detected them.

The Previous hyperlink will display the previous ten events in the list.

The Next hyperlink will display the next ten events in the list.

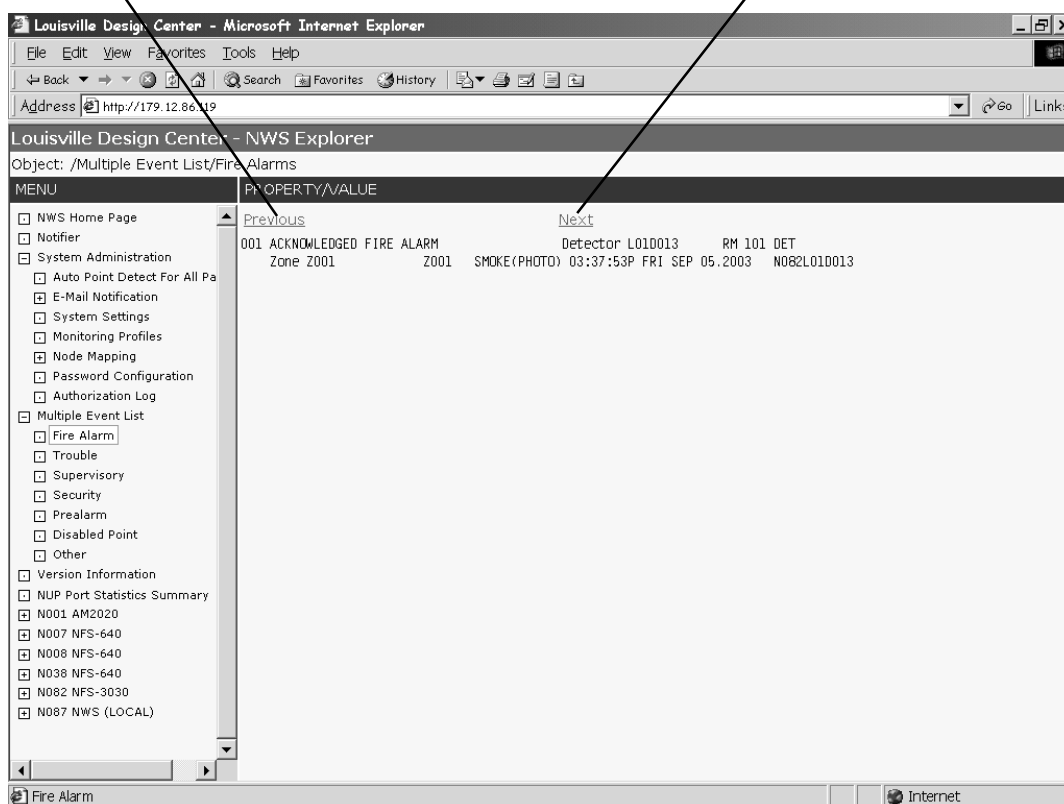


Figure 4.4-2: Multiple Event List Details

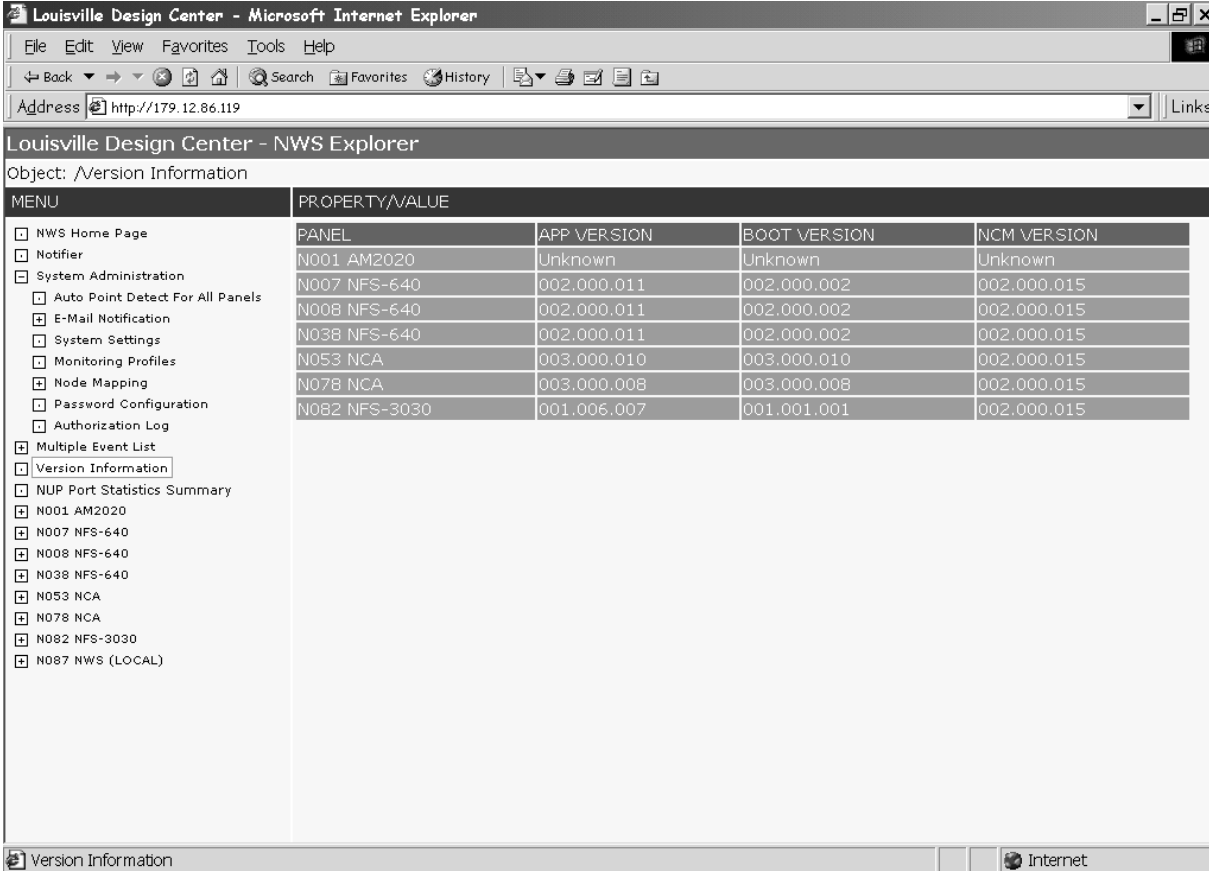
The event number	The event name	The zone	The device type, if applicable	Custom label	Extended custom label
Previous				Next	
003	FIRE ALARM	Zone 02	2002	SMOKE (ION)	11:27:40A FRI SEP 06,2002
002	FIRE ALARM	Zone 77	2077	SMOKE (PHOTO)	DETECTOR ADDE 102
001	FIRE ALARM	Zone 03	2003	SMOKE (PHOTO)	DETECTOR HALLWAY 2
				10:20:03A FRI SEP 06,2002	N045L01D010
					N040L01D002
					N040L01D090

Event details, including the date/time the event occurred.

The address where the event occurred. In this example, the Fire Alarm entry provides the exact device address.

4.5 VERSION INFORMATION

This link navigates to a screen that contains a list of panels, annunciators and related monitoring devices and the corresponding version information for them and their related network interfaces.



The screenshot shows a web browser window titled "Louisville Design Center - Microsoft Internet Explorer". The address bar displays "http://179.12.86.119". The page title is "Louisville Design Center - NWS Explorer". The object path is "/Version Information".

The main content area is divided into two sections: a left-hand menu and a right-hand table.

Menu:

- ☐ NWS Home Page
- ☐ Notifier
- ☐ System Administration
 - ☐ Auto Point Detect For All Panels
 - ☐ E-Mail Notification
 - ☐ System Settings
 - ☐ Monitoring Profiles
 - ☐ Node Mapping
 - ☐ Password Configuration
 - ☐ Authorization Log
- ☐ Multiple Event List
- ☐ Version Information
- ☐ NUP Port Statistics Summary
 - ☐ N001 AM2020
 - ☐ N007 NFS-640
 - ☐ N008 NFS-640
 - ☐ N038 NFS-640
 - ☐ N053 NCA
 - ☐ N078 NCA
 - ☐ N082 NFS-3030
 - ☐ N087 NWS (LOCAL)

Table:

PANEL	APP VERSION	BOOT VERSION	NCM VERSION
N001 AM2020	Unknown	Unknown	Unknown
N007 NFS-640	002.000.011	002.000.002	002.000.015
N008 NFS-640	002.000.011	002.000.002	002.000.015
N038 NFS-640	002.000.011	002.000.002	002.000.015
N053 NCA	003.000.010	003.000.010	002.000.015
N078 NCA	003.000.008	003.000.008	002.000.015
N082 NFS-3030	001.006.007	001.001.001	002.000.015

Figure 4.5-1: Version Information



NOTE: Only Onyx Series products (NFS-3030, NFS-640, NCA) will have version information displayed.

4.6 NUP PORT STATISTICS

There are two NUP Port Statistics pages:

- From the link menu at the left, select NUP Port Statistics Summary, and the Web Server will display a status overview of all nodes and NCMs on the NFN network (see Figure 4.6-1).
- Individual node statistics can be displayed by clicking on a node in the link menu, then selecting NUP Port Statistics from its menu (see Figure 4.6-2).

Louisville Design Center - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address http://199.62.76.119:8888 Links

Louisville Design Center - NWS Explorer

Object: /NUP Port Statistics Summary

MENU	PROPERTY/VALUE				
<input type="checkbox"/> NWS Home Page		No CACK Count	Bad CRC Count	Byte Timeout Count	Transmit Retry Max Reached Count
<input type="checkbox"/> Notifier	Panel N001	Not Available	Not Available	Not Available	Not Available
<input type="checkbox"/> System Administration	NCM N001	Not Available	Not Available	Not Available	Not Available
<input type="checkbox"/> Multiple Event List	Panel N002	Not Available	Not Available	Not Available	Not Available
<input type="checkbox"/> Version Information	NCM N002	Not Available	Not Available	Not Available	Not Available
<input type="checkbox"/> NUP Port Statistics Summary	Panel N007	1	0	0	0
<input type="checkbox"/> N001 AM2020	NCM N007	1	1	0	0
<input type="checkbox"/> N007 NWS-640	Panel N008	9	0	0	2
<input type="checkbox"/> N008 NWS-640	NCM N008	105	0	0	35
<input type="checkbox"/> N038 NWS-640	Panel N027	Not Available	Not Available	Not Available	Not Available
<input type="checkbox"/> N082 NWS-3030	NCM N027	Not Available	Not Available	Not Available	Not Available
<input type="checkbox"/> N087 NWS (LOCAL)	Panel N038	2	0	0	1
<input type="checkbox"/> N087 NWS (LOCAL)	NCM N038	52368	0	0	17456
<input type="checkbox"/> N087 NWS (LOCAL)	Panel N053	Not Available	Not Available	Not Available	Not Available
<input type="checkbox"/> N087 NWS (LOCAL)	NCM N053	Not Available	Not Available	Not Available	Not Available
<input type="checkbox"/> N087 NWS (LOCAL)	Panel N078	Not Available	Not Available	Not Available	Not Available
<input type="checkbox"/> N087 NWS (LOCAL)	NCM N078	Not Available	Not Available	Not Available	Not Available
	Panel N082	0	0	0	0
	NCM N082	9558	0	0	3186
	Panel N087	0	0	0	1
	NCM N087	4372	9	0	419

NUP Port Statistics Summary

Figure 4.6-1: NUP Port Statistics Overview



NOTE: Only Onyx Series products (NFS-3030, NFS-640, NCA) will have version information displayed.

The screenshot shows a web browser window titled "Louisville Design Center - Microsoft Internet Explorer". The address bar displays "Object: /Node 87/NUP Port Statistics". The main content area is divided into two sections: a left sidebar menu and a right table.

Left Sidebar Menu:

- ☐ NWS Home Page
- ☐ Notifier
- ☐ System Administration
- ☐ Multiple Event List
- ☐ Version Information
- ☐ NUP Port Statistics Summary
 - ☐ N001 AM2020
 - ☐ N002 AFP-300/400
 - ☐ N007 NFS-640
 - ☐ N008 NFS-640
 - ☐ N038 NFS-640
 - ☐ N053 NCA
 - ☐ N078 NCA
 - ☐ N082 NFS-3030
 - ☐ N087 NWS (LOCAL)
 - ☐ NUP Port Statistics

Right Table:

PROPERTY/VALUE				
	No CACK Count	Bad CRC Count	Byte Timeout Count	Transmit Retry Max Reached Count
Panel	0	0	0	1
NCM	36659	18	0	10251

Below the table is a button labeled "Reset Statistics".

Figure 4.6-2: Local Node NUP Port Statistics

4.7 SCREEN DETAILS AND OPTIONS FOR SPECIFIC PANELS

For any panel or device that is on the network, there will be a corresponding hyperlink option in the NFN Web Server menu list. These screens are for viewing panel/network device status and property settings. In addition to fire alarm control panels, the NFN Web Browser also allows you to view network devices such as the Network Control Station (NCS), Network Control Annunciator (NCA), and the UniNet Gateway.



NOTE: Reference the pertinent control panel user manual for property details.

MENU	PROPERTY/VALUE
<input checked="" type="checkbox"/> N082 NFS-3030	Panel Label
<input type="checkbox"/> Loop 1	
<input type="checkbox"/> Modules	
<input type="checkbox"/> L01M013 (I)	
<input type="checkbox"/> L01M017 (I)	
<input type="checkbox"/> L01M077 (O)	
<input type="checkbox"/> Panel Modules	
<input type="checkbox"/> Zones	
<input type="checkbox"/> Logic Zones	
<input type="checkbox"/> Release Zones	
<input type="checkbox"/> Trouble Zones	
<input type="checkbox"/> Custom Action Messages	
<input type="checkbox"/> Occupancy Schedule	
<input type="checkbox"/> Schedule 1	
<input type="checkbox"/> Schedule 2	
<input type="checkbox"/> Schedule 3	
<input type="checkbox"/> Schedule 4	
<input type="checkbox"/> Schedule 5	
<input type="checkbox"/> Schedule 6	
<input type="checkbox"/> Schedule 7	
<input type="checkbox"/> Schedule 8	
<input type="checkbox"/> Schedule 9	
<input type="checkbox"/> Schedule 10	
<input type="checkbox"/> Holidays	
<input type="checkbox"/> History	
<input type="checkbox"/> Alarm History	
<input type="checkbox"/> All History	
	NETWORK
	Network Address 82
	Media Channel A Threshold High
	Media Channel B Threshold High
	Media Style 7 No
	PERIPHERALS
	Remote LCD Supervision No
	PrinterFormat 80 CHAR
	Printer Supervision No
	DISPLAY
	Time Format HH:MM AM/PM
	Date Format MM/DD/YY
	Alarm Scrolling No
	LCD Backlight Mode On
	LCD Intensity 40
	SETTINGS
	Trouble Reminder One Minute
	Bell Coding Mode March Time
	Prealarm Mode Alert
	LED Blink No Blinking
	Local Control Yes
	Main Power Supply Address None

Figure 4.7-1: Panel Properties Display Sample

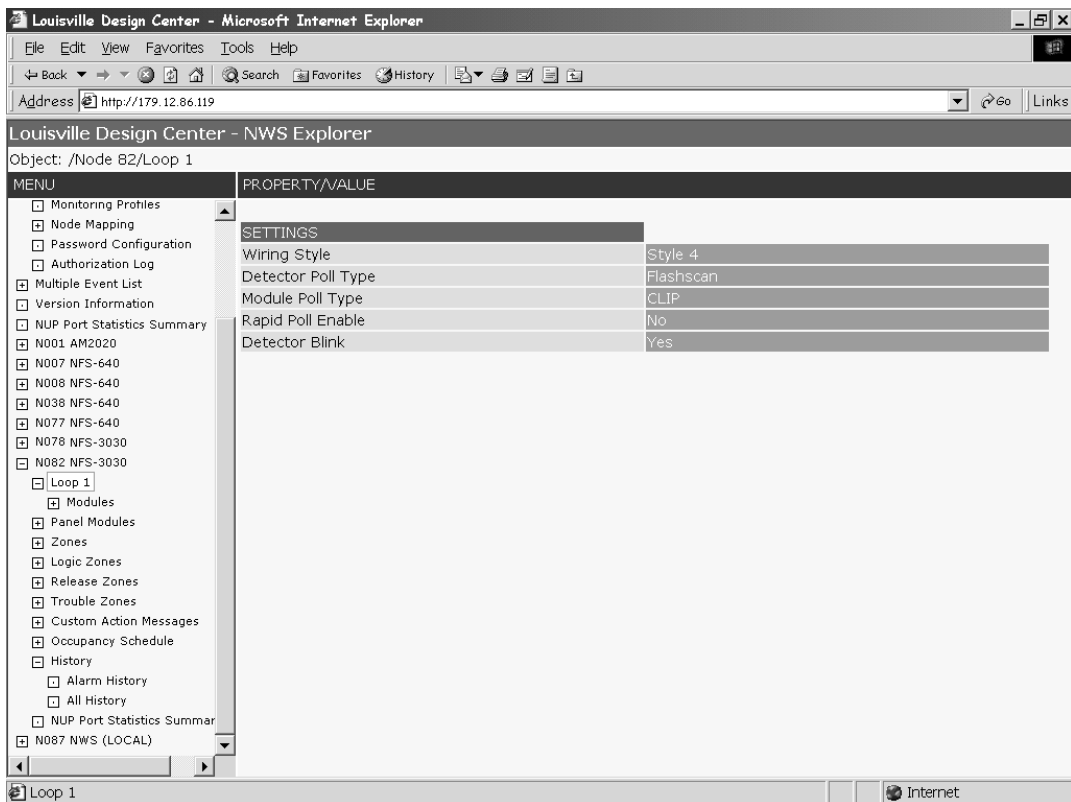


Figure 4.7-2: Loop Properties Sample Screen

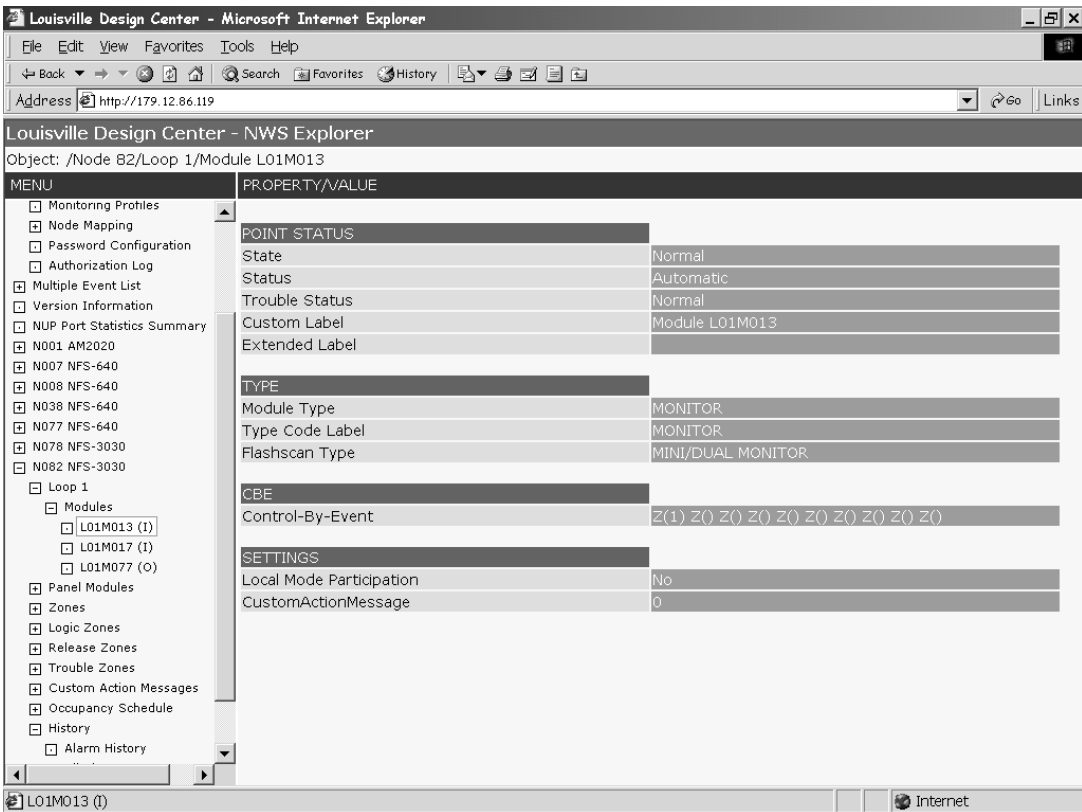


Figure 4.7-3: Module Properties Sample Screen

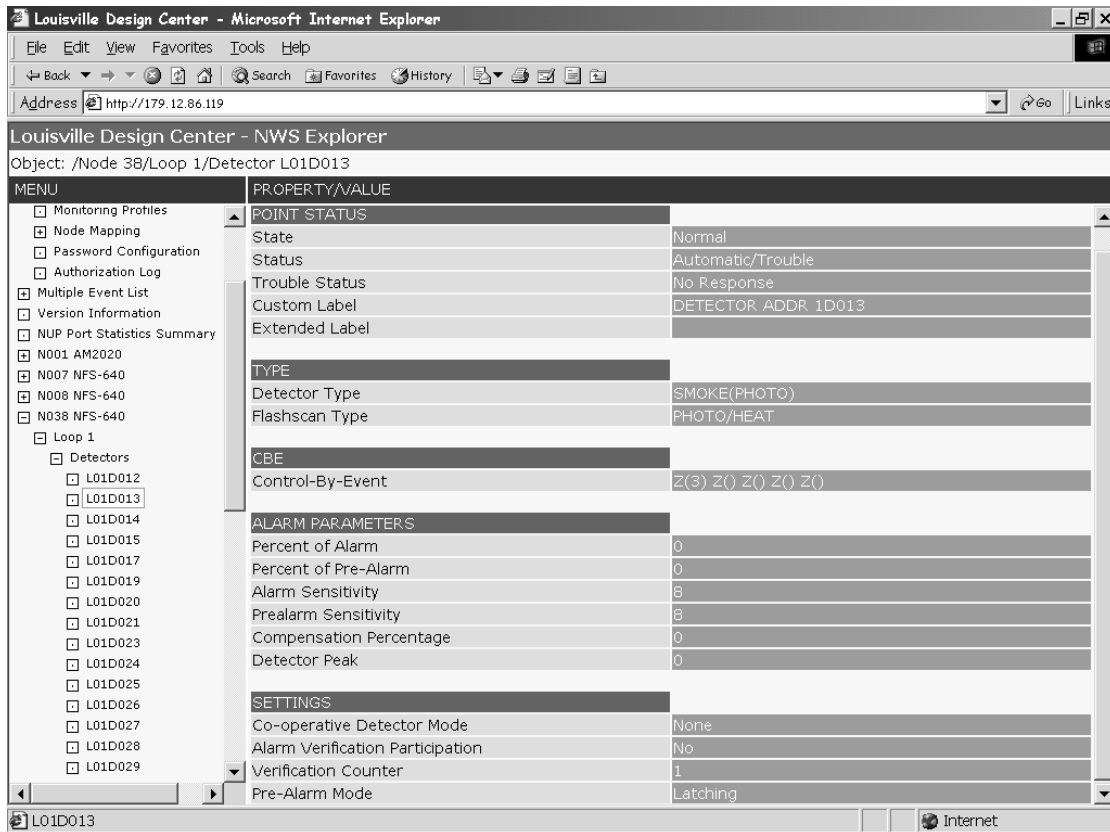


Figure 4.7-4: Detector Properties Sample Screen

Index

A

Auto Discover Points on all Panels 30, 31

B

Browser Interface 29

C

COM Port Configuration 21

Configuration Tool 21, 23

 COM Port Configuration 21

 IP ASSIGNED TO PPP (MODEM) CLIENTS 22

 IP Configuration 22

 IP FOR ROUTING BACK TO INTERNET 22

 NCM Configuration 22

 SUBNET MASK 22

 Web Server Node 21

D

Device Compatibility 8

Drop Number. *See* Node Address Change

E

E-mail Notification 32

E-mail Profiles 33

G

General Settings 35

I

Installation

 Hardware

 Network Connection 19

 NFN Web Server Assembly 15

Installation Checklist 14

IP ASSIGNED TO PPP (MODEM) CLIENTS 22

IP Configuration 22

IP FOR ROUTING BACK TO INTERNET 22

L

Login 29

M

Monitoring Profiles 36

Multiple Event List 40, 41

N

NCM Configuration 22

NCM Settings 35

Network Configuration 21

Network Connection 19

NUP Port Statistics 43

NFN Web Server Network Configuration 21

NFN Web Server PC Board Layout 15

Node Address Change 28

Node Mapping 37

P

Password Configuration 38

Passwords 29

PC Board Layout 15

Power Supply 16

R

Regulatory Standards 8

Related Documentation 7

S

Security 29

Serial Port Configuration Utility 23

Site Settings 35

SUBNET MASK 22

System Administration 30

 Monitoring Profiles 36

 Node Mapping 37

 Password Configuration 38

System Architecture 9

System Settings 35

 General Settings 35

 NCM Settings 35

 Site Settings 35

V

VeriFire Tools 23

 Connection Type 27

 IP address assigned to PPP (modem) 25

 IP address for connection to Notifier 25

 IP address for routing back to Ineternet 25

 Launching 26

 NCM Threshold and Network Styles 25

 Node Address Change 28

W

Web Server Node 21

Wiring

 Network Interface 18

 Power Supply 16

 Serial Configuration Tool 21

NOTES

NOTES

NOTES

Limited Warranty

NOTIFIER® warrants its products to be free from defects in materials and workmanship for eighteen (18) months from the date of manufacture, under normal use and service. Products are date stamped at time of manufacture. The sole and exclusive obligation of **NOTIFIER®** is to repair or replace, at its option, free of charge for parts and labor, any part which is defective in materials or workmanship under normal use and service. For products not under **NOTIFIER®** manufacturing date-stamp control, the warranty is eighteen (18) months from date of original purchase by **NOTIFIER®**'s distributor unless the installation instructions or catalog sets forth a shorter period, in which case the shorter period shall apply. This warranty is void if the product is altered, repaired or serviced by anyone other than **NOTIFIER®** or its authorized distributors or if there is a failure to maintain the products and systems in which they operate in a proper and workable manner. In case of defect, secure a Return Material Authorization form from our customer service department. Return product, transportation prepaid, to **NOTIFIER®**, 12 Clintonville Rd., Northford, Connecticut 06472-1653.

This writing constitutes the only warranty made by **NOTIFIER®** with respect to its products. **NOTIFIER®** does not represent that its products will prevent any loss by fire or otherwise, or that its products will in all cases provide the protection for which they are installed or intended. Buyer acknowledges that **NOTIFIER®** is not an insurer and assumes no risk for loss or damages or the cost of any inconvenience, transportation, damage, misuse, abuse, accident or similar incident.

NOTIFIER® GIVES NO WARRANTY, EXPRESSED OR IMPLIED, OF MERCHANTABILITY, FITNESS FOR ANY PARTICULAR PURPOSE, OR OTHERWISE WHICH EXTEND BEYOND THE DESCRIPTION ON THE FACE HEREOF. UNDER NO CIRCUMSTANCES SHALL **NOTIFIER®** BE LIABLE FOR ANY LOSS OF OR DAMAGE TO PROPERTY, DIRECT, INCIDENTAL OR CONSEQUENTIAL, ARISING OUT OF THE USE OF, OR INABILITY TO USE **NOTIFIER®** PRODUCTS. FURTHERMORE, **NOTIFIER®** SHALL NOT BE LIABLE FOR ANY PERSONAL INJURY OR DEATH WHICH MAY ARISE IN THE COURSE OF, OR AS A RESULT OF, PERSONAL, COMMERCIAL OR INDUSTRIAL USE OF ITS PRODUCTS.

This warranty replaces all previous warranties and is the only warranty made by **NOTIFIER®**. No increase or alteration, written or verbal, of the obligation of this warranty is authorized.

"**NOTIFIER**" is a registered trademark.



World Headquarters
12 Clintonville Rd.
Northford, CT 06472-1653 USA
203-484-7161
fax 203-484-7118

www.notifier.com

NOTIFIER is a **Honeywell** company

